

**CERTIFICATION AND REQUEST FOR PRIORITIZED EXAMINATION
UNDER 37 CFR 1.102(e) (Page 1 of 1)**

First Named Inventor:	Stefik	Nonprovisional Application Number (if known):	
Title of Invention:	SYSTEM AND METHOD FOR DISTRIBUTING DIGITAL CONTENT TO BE RENDERED IN ACCORDANCE WITH USAGE RIGHTS INFORMATION		

APPLICANT HEREBY CERTIFIES THE FOLLOWING AND REQUESTS PRIORITIZED EXAMINATION FOR THE ABOVE-IDENTIFIED APPLICATION.

1. The processing fee set forth in 37 CFR 1.17(i), the prioritized examination fee set forth in 37 CFR 1.17(c), and if not already paid, the publication fee set forth in 37 CFR 1.18(d) have been filed with the request. The basic filing fee, search fee, examination fee, and any required excess claims and application size fees are filed with the request or have been already been paid.
2. The application contains or is amended to contain no more than four independent claims and no more than thirty total claims, and no multiple dependent claims.
3. The applicable box is checked below:

I. ☒ Original Application (Track One) - Prioritized Examination under § 1.102(e)(1)

- i. (a) The application is an original nonprovisional utility application filed under 35 U.S.C. 111(a). This certification and request is being filed with the utility application via EFS-Web.
---OR---
(b) The application is an original nonprovisional plant application filed under 35 U.S.C. 111(a). This certification and request is being filed with the plant application in paper.
- ii. An executed oath or declaration under 37 CFR 1.63 is filed with the application.

II. ☐ Request for Continued Examination - Prioritized Examination under § 1.102(e)(2)

- i. A request for continued examination has been filed with, or prior to, this form.
- ii. If the application is a utility application, this certification and request is being filed via EFS-Web.
- iii. The application is an original nonprovisional utility application filed under 35 U.S.C. 111(a), or is a national stage entry under 35 U.S.C. 371.
- iv. This certification and request is being filed prior to the mailing of a first Office action responsive to the request for continued examination.
- v. No prior request for continued examination has been granted prioritized examination status under 37 CFR 1.102(e)(2).

Signature /Stephen M. Hertzler, Reg. 58247/	Date 2012-08-14
Name (Print/Typed) Stephen M. Hertzler	Practitioner Registration Number 58247
Note: Signatures of all the inventors or assignees of record of the entire interest or their representative(s) are required in accordance with 37 CFR 1.33 and 11.18. Please see 37 CFR 1.4(d) for the form of the signature. If necessary, submit multiple forms for more than one signature, see below*.	
☒ *Total of <u>1</u> forms are submitted.	

Privacy Act Statement

The **Privacy Act of 1974 (P.L. 93-579)** requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (*i.e.*, GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

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

Application Data Sheet 37 CFR 1.76		Attorney Docket Number	10-510-US-C73
		Application Number	
Title of Invention	SYSTEM AND METHOD FOR DISTRIBUTING DIGITAL CONTENT TO BE RENDERED IN ACCORDANCE WITH USAGE RIGHTS INFORMATION		
The application data sheet is part of the provisional or nonprovisional application for which it is being submitted. The following form contains the bibliographic data arranged in a format specified by the United States Patent and Trademark Office as outlined in 37 CFR 1.76. This document may be completed electronically and submitted to the Office in electronic format using the Electronic Filing System (EFS) or the document may be printed and included in a paper filed application.			

Secrecy Order 37 CFR 5.2

- ☐ Portions or all of the application associated with this Application Data Sheet may fall under a Secrecy Order pursuant to 37 CFR 5.2 (Paper filers only. Applications that fall under Secrecy Order may not be filed electronically.)

Applicant Information:

Applicant 1						Remove	
Applicant Authority		☒ Inventor		☐ Legal Representative under 35 U.S.C. 117		☐ Party of Interest under 35 U.S.C. 118	
Prefix	Given Name	Middle Name	Family Name		Suffix		
	Mark	J.	Stefik				
Residence Information (Select One) ☒ US Residency ☐ Non US Residency ☐ Active US Military Service							
City	Portola Valley	State/Province	CA	Country of Residenceⁱ	US		
Citizenship under 37 CFR 1.41(b)ⁱ		US					
Mailing Address of Applicant:							
Address 1		10 Portola Green Circle					
Address 2							
City	Portola Valley	State/Province	CA				
Postal Code	94028	Countryⁱ	US				
Applicant 2						Remove	
Applicant Authority		☒ Inventor		☐ Legal Representative under 35 U.S.C. 117		☐ Party of Interest under 35 U.S.C. 118	
Prefix	Given Name	Middle Name	Family Name		Suffix		
	Peter	L.T.	Pirolli				
Residence Information (Select One) ☒ US Residency ☐ Non US Residency ☐ Active US Military Service							
City	San Francisco	State/Province	CA	Country of Residenceⁱ	US		
Citizenship under 37 CFR 1.41(b)ⁱ		CA					
Mailing Address of Applicant:							
Address 1		2958 Sloat Boulevard					
Address 2							
City	San Francisco	State/Province	CA				
Postal Code	94116	Countryⁱ	US				
All Inventors Must Be Listed - Additional Inventor Information blocks may be generated within this form by selecting the Add button.						Add	

Correspondence Information:

Enter either Customer Number or complete the Correspondence Information section below.
For further information see 37 CFR 1.33(a).

- ☐ An Address is being provided for the correspondence Information of this application.

Application Data Sheet 37 CFR 1.76		Attorney Docket Number	10-510-US-C73
		Application Number	
Title of Invention	SYSTEM AND METHOD FOR DISTRIBUTING DIGITAL CONTENT TO BE RENDERED IN ACCORDANCE WITH USAGE RIGHTS INFORMATION		
Customer Number	98804		
Email Address		Add Email	Remove Email

Application Information:

Title of the Invention	SYSTEM AND METHOD FOR DISTRIBUTING DIGITAL CONTENT TO BE RENDERED IN ACCORDANCE WITH USAGE RIGHTS INFORMATION		
Attorney Docket Number	10-510-US-C73	Small Entity Status Claimed	☐
Application Type	Nonprovisional		
Subject Matter	Utility		
Suggested Class (if any)		Sub Class (if any)	
Suggested Technology Center (if any)			
Total Number of Drawing Sheets (if any)	13	Suggested Figure for Publication (if any)	

Publication Information:

☐	Request Early Publication (Fee required at time of Request 37 CFR 1.219)
☐	Request Not to Publish. I hereby request that the attached application not be published under 35 U.S.C. 122(b) and certify that the invention disclosed in the attached application has not and will not be the subject of an application filed in another country, or under a multilateral international agreement, that requires publication at eighteen months after filing.

Representative Information:

Representative information should be provided for all practitioners having a power of attorney in the application. Providing this information in the Application Data Sheet does not constitute a power of attorney in the application (see 37 CFR 1.32). Enter either Customer Number or complete the Representative Name section below. If both sections are completed the Customer Number will be used for the Representative Information during processing.			
Please Select One:	☒ Customer Number	☐ US Patent Practitioner	☐ Limited Recognition (37 CFR 11.9)
Customer Number	98804		

Domestic Benefit/National Stage Information:

This section allows for the applicant to either claim benefit under 35 U.S.C. 119(e), 120, 121, or 365(c) or indicate National Stage entry from a PCT application. Providing this information in the application data sheet constitutes the specific reference required by 35 U.S.C. 119(e) or 120, and 37 CFR 1.78(a)(2) or CFR 1.78(a)(4), and need not otherwise be made part of the specification.			
Prior Application Status	Pending	Remove	
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)
	Continuation of	13584782	2012-08-13
Prior Application Status	Pending	Remove	
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)
13584782	Continuation of	11304793	2005-12-16

Application Data Sheet 37 CFR 1.76		Attorney Docket Number		10-510-US-C73	
		Application Number			
Title of Invention		SYSTEM AND METHOD FOR DISTRIBUTING DIGITAL CONTENT TO BE RENDERED IN ACCORDANCE WITH USAGE RIGHTS INFORMATION			
Prior Application Status		Patented		Remove	
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)	Patent Number	Issue Date (YYYY-MM-DD)
11304793	Division of	11135352	2005-05-24	7266529	2007-09-04
Prior Application Status		Patented		Remove	
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)	Patent Number	Issue Date (YYYY-MM-DD)
11135352	Continuation of	10322759	2002-12-19	6898576	2005-05-24
Prior Application Status		Patented		Remove	
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)	Patent Number	Issue Date (YYYY-MM-DD)
10322759	Continuation of	09778001	2001-02-07	6708157	2004-03-16
Prior Application Status		Patented		Remove	
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)	Patent Number	Issue Date (YYYY-MM-DD)
09778001	Division of	08967084	1997-11-10	6236971	2001-05-22
Prior Application Status		Abandoned		Remove	
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)		
08967084	Continuation of	08344760	1994-11-23		
Additional Domestic Benefit/National Stage Data may be generated within this form by selecting the Add button. Add					

Foreign Priority Information:

This section allows for the applicant to claim benefit of foreign priority and to identify any prior foreign application for which priority is not claimed. Providing this information in the application data sheet constitutes the claim for priority as required by 35 U.S.C. 119(b) and 37 CFR 1.55(a).			
Remove			
Application Number	Country ⁱ	Parent Filing Date (YYYY-MM-DD)	Priority Claimed
			☐ Yes ☒ No
Additional Foreign Priority Data may be generated within this form by selecting the Add button. Add			

Assignee Information:

Providing this information in the application data sheet does not substitute for compliance with any requirement of part 3 of Title 37 of the CFR to have an assignment recorded in the Office.	
Remove	
Assignee 1	
If the Assignee is an Organization check here. ☒	
Organization Name	ContentGuard Holdings, Inc.

Application Data Sheet 37 CFR 1.76		Attorney Docket Number	10-510-US-C73
		Application Number	
Title of Invention	SYSTEM AND METHOD FOR DISTRIBUTING DIGITAL CONTENT TO BE RENDERED IN ACCORDANCE WITH USAGE RIGHTS INFORMATION		

Mailing Address Information:			
Address 1		103 Foulk Road, Suite 200-M	
Address 2			
City	Wilmington	State/Province	DE
Country i	US	Postal Code	19803
Phone Number		Fax Number	
Email Address			
Additional Assignee Data may be generated within this form by selecting the Add button.			
			Add

Signature:

A signature of the applicant or representative is required in accordance with 37 CFR 1.33 and 10.18. Please see 37 CFR 1.4(d) for the form of the signature.					
Signature	/Stephen M. Hertzler, Reg. No. 58247/			Date (YYYY-MM-DD)	2012-08-14
First Name	Stephen M.	Last Name	Hertzler	Registration Number	58247

This collection of information is required by 37 CFR 1.76. 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 1.14. This collection is estimated to take 23 minutes to complete, including gathering, preparing, and submitting the completed application data sheet 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.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these records.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Please type a plus sign (+) inside this box → [+]

PTO/SB/01 (12-97)

Approved for use through 9/30/00. OMB 0651-0032

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 contains a valid OBM control number.

DECLARATION FOR UTILITY OR DESIGN PATENT APPLICATION (37 CFR 1.63)		Attorney Docket Number	111325-89	
		First Named Inventor	Mark J. Stefik et al.	
		COMPLETE IF KNOWN		
		Application Number	10/015,952	
		Filing Date	December 17, 2001	
		Group Art Unit	2161	
		Examiner Name	Not yet assigned	
☐ Declaration Submitted With Initial Filing OR ☒ Declaration Submitted after Initial Filing (surcharge (37 CFR 1.16(d)) required)				
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: <u>Usage Rights Grammar And Digital Works Having Usage Rights Created With The Grammar</u> <i>(Title of the Invention)</i> the specification of which ☐ is attached hereto OR ☒ was filed on (MM/DD/YYYY) 12/17/2001 As United States Application Number or PCT International Application Number 10/015,952 And was amended on (MM/DD/YYYY) _____ (If applicable). I hereby state that I have reviewed and understand the contents of the above identified specification, including the claims, as amended by any amendment specifically referred to above. I acknowledge the duty to disclose information which is material to patentability as defined in 37 CFR 1.56.				
I hereby claim foreign priority benefits under 35 U.S.C. 119(a)-(d) or 365(b) of any foreign application(s) for patent or inventor's certificate, or 365(a) of any PCT international application which designated at least one country other than the United States of America, listed below and have also identified below, by checking the box, any foreign application for patent or inventor's certificate, or of any PCT international application having a filing date before that of the application on which priority is claimed.				
Prior Foreign Application Number(s)	Country	Foreign Filing Date (MM/DD/YYYY)	Priority Not Claimed	Certified Copy Attached YES No
			☐ ☐ ☐ ☐	☐ ☐ ☐ ☐
☐ Additional foreign application numbers are listed on a supplemental priority data sheet PTO/SB/02B attached hereto:				
I hereby claim the benefit under 35 U.S.C. 119(e) of any United States provisional application(s) listed below.				
Application Number(s)	Filing Date (MM/DD/YYYY)	☐ Additional provisional application Numbers are listed on a supplemental priority data sheet PTO/SB/02B attached hereto.		

[Page 1 of 3]

Burden Hour Statement: This form is estimated to take 0.4 hours to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, Patent and Trademark Office, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissions for Patents, Washington, DC 20231.

BEST AVAILABLE COPY

Please type a plus sign (+) inside this box → [+]

PTO/SB/01 (12-97)

Approved for use through 9/30/00. OMB 0651-0032

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 contains a valid OBM control number.

DECLARATION – Utility or Design Patent Application

I hereby claim the benefit under 35 U.S.C. 120 of any United States application(s), or 365© of any PT international application designating the United States of America, listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States or PCT International application in the manner provided by the first paragraph of 35 U.S.C. 112, I acknowledge the duty to disclose information which is material to patentability as defined in 37 CFR 1.56 which became available between the filing date of the prior application and the national or PCT international filing date of this application.

U.S. Parent Application or PCT Parent Number	Parent Filing Date (MM/DD/YYYY)	Parent Patent Number (if applicable)
This Application is a Continuation of USSN 09/778,001 which is a Divisional Application of USSN 08/967,084 which is a Continuation of USSN 08/344,760	02/07/2001 11/10/1997 11/23/1994	 6,236,971 now abandoned

[] Additional U.S. or PCT international application are listed on a supplemental priority date sheet PTO/SB/02B attached hereto.

As a named inventor, I hereby appoint the following registered practitioner(s) to prosecute this application and to transact all business in the Patent and Trademark Office connected therewith: [X] Customer Number 22204

OR

[X] Registered practitioner(s) name/registration number listed below.

Name	Registration Number	Name	Registration Number
Stuart J. Friedman	24,312	Eric J. Robinson	38,285
Charles M. Leedom, Jr.	26,477	Daniel S. Song	43,143
David S. Safran	27,997	Marc S. Kaufman	35,212
Thomas W. Cole	28,290	Corinne R. Gorski	34,339
Donald R. Studebaker	32,815	Jason H. Vick	45,285
Jeffrey L. Costellia	35,483	Luan C. Do	38,434
Tim L. Brackett, Jr.	36,092		

Direct all correspondence to: [X] Customer Number 22204

Name: Marc S. Kaufman

Firm: NIXON PEABODY LLP

Address: 8180 Greensboro Drive, Suite 800

City: McLean

State: VA

ZIP: 22102

Country: United States

Telephone: (703) 790-9110

FAX: (703) 883-0370

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 18 U.S.C. 1001 and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

Name of Sole or First Inventor:

[] A petition has been filed for this unsigned inventor.

Given Name (first and middle (if any))	Family Name or Surname
Mark J.	STEFIK

Inventor's Signature: *Mark J. Stefik*

Date:

Mailing Address (Street or P.O. Box): 55 Big Tree Way 10 Portola Green Circle

City: Woodside Portola Valley

State: California

ZIP: 94062 94028

Country: US

Residence: City:

State:

Country:

Citizenship: USA

[] Additional inventors are being named on the _____ Supplemental Additional Inventor(s) sheet(s) PTO/SB/02A attached hereto.

[Page 2 of 3]

BEST AVAILABLE COPY

Please type a plus sign (+) inside this box → [+]

PTO/SB/02A (10-00)

Approved for use through 10/31/2002. OMB 0651-0032
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 contains a valid OBM control number.

DECLARATION	ADDITIONAL INVENTOR(S) Supplemental Sheet Page ____ of ____

Name of Additional Joint Inventor, if any:		☐ A petition has been filed for this unsigned inventor	
Given Name Peter L.T.		Family Name Or Surname PIROLI	
Inventor's Signature <i>Peter Piroli</i>		Date 2/5/02	
Mailing Address (Street or P.O. Box): 44 Wildwood Place 2958 Slout Blvd			
City: San Francisco		State: California	ZIP: 94130 Country: US
Residence: City:		State:	Country:
Citizenship: Canadian			
Name of Additional Joint Inventor, if any:		☐ A petition has been filed for this unsigned inventor	
Given Name		Family Name Or Surname	
Inventor's Signature		Date	
Mailing Address (Street or P.O. Box):			
City:		State:	ZIP: Country:
Residence: City:		State:	Country:
Citizenship:			
Name of Additional Joint Inventor, if any:		☐ A petition has been filed for this unsigned inventor	
Given Name		Family Name Or Surname	
Inventor's Signature		Date	
Mailing Address (Street or P.O. Box):			
City:		State:	ZIP: Country:
Residence: City:		State:	Country:
Citizenship:			

Burden Hour Statement: This form is estimated to take 21 minutes to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, Washington, DC 20231.

[Page 3 of 3]

BEST AVAILABLE COPY

**SYSTEM AND METHOD FOR DISTRIBUTING DIGITAL CONTENT TO BE
RENDERED IN ACCORDANCE WITH USAGE RIGHTS INFORMATION.**

CROSS REFERENCE TO RELATED APPLICATIONS

[0001] This application is a continuation of U.S. Application No. 13/584,782, filed August 13, 2012, which is a continuation of U.S. Application No. 11/304,793, filed December 16, 2005, which is a divisional of U.S. Application No. 11/135,352, filed May 24, 2005, now U.S. Patent No. 7,266,529, which is a continuation of U.S. Application No. 10/322,759, filed December 19, 2002, now U.S. Patent No. 6,898,576, which is a continuation of U.S. Application No. 09/778,001, filed February 7, 2001, now U.S. Patent No. 6,708,157, which is a divisional of U.S. Application No. 08/967,084, filed November 10, 1997, now U.S. Patent No. 6,236,971, which is a continuation of U.S. Application No. 08/344,760, filed November 23, 1994, now abandoned, the entire disclosures of all of which are hereby incorporated by reference herein.

Field of the Invention

[0002] The present invention relates to the field of distribution and usage rights enforcement for digitally encoded works.

BACKGROUND OF THE INVENTION

[0003] A fundamental issue facing the publishing and information industries as they consider electronic publishing is how to prevent the unauthorized and unaccounted distribution or usage of electronically published materials. Electronically published materials are typically distributed in a digital form and recreated on a computer based system having the capability to recreate the materials. Audio and video recordings, software, books and multimedia works are all being electronically published. Companies in these industries receive royalties for each accounted for delivery of the materials, e.g. the sale of an audio CD at a retail outlet. Any unaccounted distribution of a work results in an unpaid royalty (e.g. copying the audio recording CD to another digital medium.)

[0004] The ease in which electronically published works can be “perfectly” reproduced and distributed is a major concern. The transmission of digital works over networks is commonplace. One such widely used network is the Internet. The Internet is a widespread network facility by which computer users in many universities, corporations and government entities communicate and trade ideas and information. Computer bulletin boards

found on the Internet and commercial networks such as CompuServ and Prodigy allow for the posting and retrieving of digital information. Information services such as Dialog and LEXIS/NEXIS provide databases of current information on a wide variety of topics. Another factor which will exacerbate the situation is the development and expansion of the National Information Infrastructure (the NII). It is anticipated that, as the NII grows, the transmission of digital works over networks will increase many times over. It would be desirable to utilize the NII for distribution of digital works without the fear of widespread unauthorized copying.

[0005] The most straightforward way to curb unaccounted distribution is to prevent unauthorized copying and transmission. For existing materials that are distributed in digital form, various safeguards are used. In the case of software, copy protection schemes which limit the number of copies that can be made or which corrupt the output when copying is detected have been employed. Another scheme causes software to become disabled after a predetermined period of time has lapsed. A technique used for workstation based software is to require that a special hardware device must be present on the workstation in order for the software to run, e.g., see U.S. Pat. No. 4,932,054 entitled "Method and Apparatus for Protecting Computer Software Utilizing Coded Filter Network in Conjunction with an Active Coded Hardware Device." Such devices are provided with the software and are commonly referred to as dongles.

[0006] Yet another scheme is to distribute software, but which requires a "key" to enable its use. This is employed in distribution schemes where "demos" of the software are provided on a medium along with the entire product. The demos can be freely used, but in order to use the actual product, the key must be purchased. These schemes do not hinder copying of the software once the key is initially purchased.

[0007] A system for ensuring that licenses are in place for using licensed products is described in PCT Publication WO 93/01550 to Griswold entitled "License Management System and Method." The licensed product may be any electronically published work but is most effective for use with works that are used for extended periods of time such as software programs. Griswold requires that the licensed product contain software to invoke a license check monitor at predetermined time intervals. The license check monitor generates request datagrams which identify the licensee. The request datagrams are sent to a license control system over an appropriate communication facility. The license control system then checks the datagram to determine if the datagram is from a valid licensee. The license control system then sends a reply datagram to the license check monitor indicating denial or approval of

usage. The license control system will deny usage in the event that request datagrams go unanswered after a predetermined period of time (which may indicate an unauthorized attempt to use the licensed product). In this system, usage is managed at a central location by the response datagrams. So for example if license fees have not been paid, access to the licensed product is terminated.

[0008] It is argued by Griswold that the described system is advantageous because it can be implemented entirely in software. However, the system described by Griswold has limitations. An important limitation is that during the use of the licensed product, the user must always be coupled to an appropriate communication facility in order to send and receive datagrams. This creates a dependency on the communication facility. So if the communication facility is not available, the licensed product cannot be used. Moreover, some party must absorb the cost of communicating with the license server.

[0009] A system for controlling the distribution of digitally encoded books is embodied in a system available from VPR Systems, LTD. of St. Louis, Miss. The VPR system is self-contained and is comprised of: (1) point of sale kiosks for storing and downloading of books, (2) personal storage mediums (cartridges) to which the books are downloaded, and (3) readers for viewing the book. In a purchase transaction, a purchaser will purchase a voucher card representing the desired book. The voucher will contain sufficient information to identify the book purchased and perhaps some demographic information relating to the sales transaction. To download the book, the voucher and the cartridge are inserted into the kiosk.

[0010] The VPR system may also be used as a library. In such an embodiment, the kiosk manages the number of “copies” that may be checked out at one time. Further, the copy of the book is erased from the user’s cartridge after a certain check-out time has expired. However, individuals cannot loan books because the cartridges may only be used with the owner’s reader.

[0011] The foregoing distribution and protection schemes operate in part by preventing subsequent distribution of the work. While this certainly prevents unauthorized distributions, it does so by sacrificing the potential for subsequent revenue bearing uses. For example, it may be desirable to allow the lending of a purchased work to permit exposure of the work to potential buyers. Another example would be to permit the creation of a derivative work for a fee. Yet another example would be to permit copying the work for a fee

(essentially purchasing it). Thus, it would be desirable to provide flexibility in how the owner of a digital work may allow it to be distributed.

[0012] While flexibility in distribution is a concern, the owners of a work want to make sure they are paid for such distributions. In U.S. Pat. No. 4,977,594 to Shear, entitled “Database Usage Metering and Protection System and Method,” a system for metering and billing for usage of information distributed on a CD-ROM is described. The system requires the addition of a billing module to the computer system. The billing module may operate in a number of different ways. First, it may periodically communicate billing data to a central billing facility, whereupon the user may be billed. Second, billing may occur by disconnecting the billing module and the user sending it to a central billing facility where the data is read and a user bill generated.

[0013] U.S. Pat. No. 5,247,575, Sprague et al., entitled “Information Distribution System”, describes an information distribution system which provides and charges only for user selected information. A plurality of encrypted information packages (IPs) are provided at the user site, via high and/or low density storage media and/or by broadcast transmission. Some of the IPs may be of no interest to the user. The IPs of interest are selected by the user and are decrypted and stored locally. The IPs may be printed, displayed or even copied to other storage media. The charges for the selected IP's are accumulated within a user apparatus and periodically reported by telephone to a central accounting facility. The central accounting facility also issues keys to decrypt the IPs. The keys are changed periodically. If the central accounting facility has not issued a new key for a particular user station, the station is unable to retrieve information from the system when the key is changed.

[0014] A system available from Wave Systems Corp. of Princeton, N.Y., provides for metering of software usage on a personal computer. The system is installed onto a computer and collects information on what software is in use, encrypts it and then transmits the information to a transaction center. From the transaction center, a bill is generated and sent to the user. The transaction center also maintains customer accounts so that licensing fees may be forwarded directly to the software providers. Software operating under this system must be modified so that usage can be accounted.

[0015] Known techniques for billing do not provide for billing of copies made of the work. For example, if data is copied from the CD-ROM described in Shear, any subsequent use of the copy of the information cannot be metered or billed. In other words, the means for

billing runs with the media rather than the underlying work. It would be desirable to have a distribution system where the means for billing is always transported with the work.

SUMMARY OF THE INVENTION

[0016] A method, system and software for associating usage rights with digital content is provided, including creating usage rights from a grammar, the usage rights specifying a manner of use indicating purposes for which the digital content is used and/or distributed by an authorized party; associating the usage rights with a digital content; processing a usage transaction specifying the usage rights to determine if access to the digital content is granted; and storing the usage rights in a distributed repository. The usage rights also specify one or more conditions which must be satisfied before the manner of use is exercised. The creating includes selecting symbols from a first set of predetermined symbols to define a valid sequence of symbols to indicate the manner of use, selecting one or more symbols from a second set of predetermined symbols to define a valid sequence of symbols to indicate the conditions.

[0017] In further embodiments, a system for controlling the distribution and use of digital works using digital tickets is disclosed. A ticket is an indicator that the ticket holder has already paid for or is otherwise entitled to some specified right, product or service. In the present invention, a “digital ticket” is used to enable the ticket holder to exercise usage rights specifying the requirement of the digital ticket. Usage rights are used to define how a digital work may be used or distributed. Specific instances of usage rights are used to indicate a particular manner of use or distribution. A usage right may specify a digital ticket which must be present before the right may be exercised. For example, a digital ticket may be specified in a Copy right of a digital work, so that exercise of the Copy right requires the party that desires a copy of the digital work be in possession of the necessary digital ticket. After a copy of the digital work is successfully sent to the requesting party, the digital ticket is “punched” to indicate that a copy of the digital work has been made. When the ticket is “punched” a predetermined number of times, it may no longer be used.

[0018] Digital works are stored in repositories. Repositories enforce the usage rights for digital works. Each repository has a “generic ticket agent” which punches tickets. In some instances only the generic ticket agent is necessary. In other instances, punching by a “special ticket agent” residing on another repository may be desired. Punching by a “special ticket agent” enables greater security and control of the digital work. For example, it can help

prevent digital ticket forgery. Special ticket agents are also useful in situations where an external database needs to be updated or checked.

[0019] A digital ticket is merely an instance of a digital work. Thus, a digital ticket may be distributed among repositories in the same fashion as other digital works.

[0020] A digital ticket may be used in many commercial scenarios such as in the purchase of software and prepaid upgrades. A digital ticket may also be used to limit the number of times that a right may be exercised. For example, a user may purchase a copy of a digital work, along with the right to make up to 5 Copies. In this case, the Copy right would have associated therewith a digital ticket that can be punched up to 5 times. Other such commercial scenarios will become apparent from the detailed description.

BRIEF DESCRIPTION OF THE DRAWINGS

[0021] FIG. 1 is a flowchart illustrating a simple instantiation of the operation of the currently preferred embodiment of the present invention.

[0022] FIG. 2 is a block diagram illustrating the various repository types and the repository transaction flow between them in the currently preferred embodiment of the present invention.

[0023] FIG. 3 is a block diagram of a repository coupled with a credit server in the currently preferred embodiment of the present invention.

[0024] FIGS. 4a and 4b are examples of rendering systems as may be utilized in the currently preferred embodiment of the present invention.

[0025] FIG. 5 illustrates a contents file layout for a digital work as may be utilized in the currently preferred embodiment of the present invention.

[0026] FIG. 6 illustrates a contents file layout for an individual digital work of the digital work of FIG. 5 as may be utilized in the currently preferred embodiment of the present invention.

[0027] FIG. 7 illustrates the components of a description block of the currently preferred embodiment of the present invention.

[0028] FIG. 8 illustrates a description tree for the contents file layout of the digital work illustrated in FIG. 5.

[0029] FIG. 9 illustrates a portion of a description tree corresponding to the individual digital work illustrated in FIG. 6.

[0030] FIG. 10 illustrates a layout for the rights portion of a description block as may be utilized in the currently preferred embodiment of the present invention.

[0031] FIG. 11 is a description tree wherein certain d-blocks have PRINT usage rights and is used to illustrate “strict” and “lenient” rules for resolving usage rights conflicts.

[0032] FIG. 12 is a block diagram of the hardware components of a repository as are utilized in the currently preferred embodiment of the present invention.

[0033] FIG. 13 is a block diagram of the functional (logical) components of a repository as are utilized in the currently preferred embodiment of the present invention.

[0034] FIG. 14 is diagram illustrating the basic components of a usage right in the currently preferred embodiment of the present invention.

[0035] FIG. 15 lists the usage rights grammar of the currently preferred embodiment of the present invention.

[0036] FIG. 16 is a flowchart illustrating the steps of certificate delivery, hotlist checking and performance testing as performed in a registration transaction as may be performed in the currently preferred embodiment of the present invention.

[0037] FIG. 17 is a flowchart illustrating the steps of session information exchange and clock synchronization as may be performed in the currently preferred embodiment of the present invention, after each repository in the registration transaction has successfully completed the steps described in FIG. 16.

[0038] FIG. 18 is a flowchart illustrating the basic flow for a usage transaction, including the common opening and closing step, as may be performed in the currently preferred embodiment of the present invention.

[0039] FIG. 19 is a state diagram of server and client repositories in accordance with a transport protocol followed when moving a digital work from the server to the client repositories, as may be performed in the currently preferred embodiment of the present invention.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

Overview

[0040] A system for controlling use and distribution of digital works is disclosed. The present invention is directed to supporting commercial transactions involving digital works. The transition to digital works profoundly and fundamentally changes how creativity and commerce can work. It changes the cost of transporting or storing works because digital property is almost “massless.” Digital property can be transported at electronic speeds and requires almost no warehousing. Keeping an unlimited supply of virtual copies on hand requires essentially no more space than keeping one copy on hand. The digital medium also lowers the costs of alteration, reuse and billing.

[0041] There is a market for digital works because creators are strongly motivated to reuse portions of digital works from others rather than creating their own completely. This is because it is usually so much easier to use an existing stock photo or music clip than to create a new one from scratch.

[0042] Herein the terms “digital work”, “work” and “content” refer to any work that has been reduced to a digital representation. This would include any audio, video, text, or multimedia work and any accompanying interpreter (e.g. software) that may be required for recreating the work. The term composite work refers to a digital work comprised of a collection of other digital works. The term “usage rights” or “rights” is a term which refers to rights granted to a recipient of a digital work. Generally, these rights define how a digital work can be used and if it can be further distributed. Each usage right may have one or more specified conditions which must be satisfied before the right may be exercised. Appendix 1 provides a Glossary of the terms used herein.

[0043] A key feature of the present invention is that usage rights are permanently “attached” to the digital work. Copies made of a digital work will also have usage rights attached. Thus, the usage rights and any associated fees assigned by a creator and subsequent distributor will always remain with a digital work.

[0044] The enforcement elements of the present invention are embodied in repositories. Among other things, repositories are used to store digital works, control access to digital works, bill for access to digital works and maintain the security and integrity of the system.

[0045] The combination of attached usage rights and repositories enable distinct advantages over prior systems. As noted in the prior art, payment of fees are primarily for the initial access. In such approaches, once a work has been read, computational control over that

copy is gone. Metaphorically, “the content genie is out of the bottle and no more fees can be billed.” In contrast, the present invention never separates the fee descriptions from the work. Thus, the digital work genie only moves from one trusted bottle (repository) to another, and all uses of copies are potentially controlled and billable.

[0046] FIG. 1 is a high level flowchart omitting various details but which demonstrates the basic operation of the present invention. Referring to FIG. 1, a creator creates a digital work, step 101. The creator will then determine appropriate usage rights and fees, attach them to the digital work, and store them in Repository 1, step 102. The determination of appropriate usage rights and fees will depend on various economic factors. The digital work remains securely in Repository 1 until a request for access is received. The request for access begins with a session initiation by another repository. Here a Repository 2 initiates a session with Repository 1, step 103. As will be described in greater detail below, this session initiation includes steps which help to insure that the respective repositories are trustworthy. Assuming that a session can be established, Repository 2 may then request access to the Digital Work for a stated purpose, step 104. The purpose may be, for example, to print the digital work or to obtain a copy of the digital work. The purpose will correspond to a specific usage right. In any event, Repository 1 checks the usage rights associated with the digital work to determine if the access to the digital work may be granted, step 105. The check of the usage rights essentially involves a determination of whether a right associated with the access request has been attached to the digital work and if all conditions associated with the right are satisfied. If the access is denied, repository 1 terminates the session with an error message, step 106. If access is granted, repository 1 transmits the digital work to repository 2, step 107. Once the digital work has been transmitted to repository 2, repository 1 and 2 each generate billing information for the access which is transmitted to a credit server, step 108. Such double billing reporting is done to insure against attempts to circumvent the billing process.

[0047] FIG. 2 illustrates the basic interactions between repository types in the present invention. As will become apparent from FIG. 2, the various repository types will serve different functions. It is fundamental that repositories will share a core set of functionality which will enable secure and trusted communications. Referring to FIG. 2, a repository 201 represents the general instance of a repository. The repository 201 has two modes of operation; a server mode and a requester mode. When in the server mode, the repository will be receiving and processing access requests to digital works. When in the requester mode, the

repository will be initiating requests to access digital works. Repository 201 is general in the sense that its primary purpose is as an exchange medium for digital works. During the course of operation, the repository 201 may communicate with a plurality of other repositories, namely authorization repository 202, rendering repository 203 and master repository 204. Communication between repositories occurs utilizing a repository transaction protocol 205.

[0048] Communication with an authorization repository 202 may occur when a digital work being accessed has a condition requiring an authorization. Conceptually, an authorization is a digital certificate such that possession of the certificate is required to gain access to the digital work. An authorization is itself a digital work that can be moved between repositories and subjected to fees and usage rights conditions. An authorization may be required by both repositories involved in an access to a digital work.

[0049] Communication with a rendering repository 203 occurs in connection with the rendering of a digital work. As will be described in greater detail below, a rendering repository is coupled with a rendering device (e.g. a printer device) to comprise a rendering system.

[0050] Communication with a master repository 205 occurs in connection with obtaining an identification certificate. Identification certificates are the means by which a repository is identified as “trustworthy”. The use of identification certificates is described below with respect to the registration transaction.

[0051] FIG. 3 illustrates the repository 201 coupled to a credit server 301. The credit server 301 is a device which accumulates billing information for the repository 201. The credit server 301 communicates with repository 201 via billing transactions 302 to record billing transactions. Billing transactions are reported to a billing clearinghouse 303 by the credit server 301 on a periodic basis. The credit server 301 communicates to the billing clearinghouse 303 via clearinghouse transactions 304. The clearinghouse transactions 304 enable a secure and encrypted transmission of information to the billing clearinghouse 303.

RENDERING SYSTEMS

[0052] A rendering system is generally defined as a system comprising a repository and a rendering device which can render a digital work into its desired form. Examples of a rendering system may be a computer system, a digital audio system, or a printer. A rendering system has the same security features as a repository. The coupling of a rendering repository with the rendering device may occur in a manner suitable for the type of rendering device.

[0053] FIG. 4a illustrates a printer as an example of a rendering system. Referring to FIG. 4, printer system 401 has contained therein a printer repository 402 and a print device 403. It should be noted that the dashed line defining printer system 401 defines a secure system boundary. Communications within the boundary is assumed to be secure. Depending on the security level, the boundary also represents a barrier intended to provide physical integrity. The printer repository 402 is an instantiation of the rendering repository 205 of FIG. 2. The printer repository 402 will in some instances contain an ephemeral copy of a digital work which remains until it is printed out by the print engine 403. In other instances, the printer repository 402 may contain digital works such as fonts, which will remain and can be billed based on use. This design assures that all communication lines between printers and printing devices are encrypted, unless they are within a physically secure boundary. This design feature eliminates a potential “fault” point through which the digital work could be improperly obtained. The printer device 403 represents the printer components used to create the printed output.

[0054] Also illustrated in FIG. 4a is the repository 404. The repository 404 is coupled to the printer repository 402. The repository 404 represents an external repository which contains digital works.

[0055] FIG. 4b is an example of a computer system as a rendering system. A computer system may constitute a “multi-function” device since it may execute digital works (e.g. software programs) and display digital works (e.g. a digitized photograph). Logically, each rendering device can be viewed as having its own repository, although only one physical repository is needed. Referring to FIG. 4b, a computer system 410 has contained therein a display/execution repository 411. The display/execution repository 411 is coupled to display device, 412 and execution device 413. The dashed box surrounding the computer system 410 represents a security boundary within which communications are assumed to be secure. The display/execution repository 411 is further coupled to a credit server 414 to report any fees to be billed for access to a digital work and a repository 415 for accessing digital works stored therein.

STRUCTURE OF DIGITAL WORKS

[0056] Usage rights are attached directly to digital works. Thus, it is important to understand the structure of a digital work. The structure of a digital work, in particular composite digital works, may be naturally organized into an acyclic structure such as a hierarchy. For example, a magazine has various articles and photographs which may have

been created and are owned by different persons. Each of the articles and photographs may represent a node in a hierarchical structure. Consequently, controls, i.e. usage rights, may be placed on each node by the creator. By enabling control and fee billing to be associated with each node, a creator of a work can be assured that the rights and fees are not circumvented.

[0057] In the currently preferred embodiment, the file information for a digital work is divided into two files: a “contents” file and a “description tree” file. From the perspective of a repository, the “contents” file is a stream of addressable bytes whose format depends completely on the interpreter used to play, display or print the digital work. The description tree file makes it possible to examine the rights and fees for a work without reference to the content of the digital work. It should be noted that the term description tree as used herein refers to any type of acyclic structure used to represent the relationship between the various components of a digital work.

[0058] FIG. 5 illustrates the layout of a contents file. Referring to FIG. 5, a digital work 509 is comprised of story A 510, advertisement 511, story B 512 and story C 513. It is assumed that the digital work is stored starting at a relative address of 0. Each of the parts of the digital work are stored linearly so that story A 510 is stored at approximately addresses 0-30,000, advertisement 511 at addresses 30,001-40,000, story B 512 at addresses 40,001-60,000 and story C 513 at addresses 60,001-85K. The detail of story A 510 is illustrated in FIG. 6. Referring to FIG. 6, the story A 510 is further broken down to show text 614 stored at address 0-1500, soldier photo 615 at addresses 1501-10,000, graphics 616 stored at addresses 10,001-25,000 and sidebar 617 stored address 25,001-30,000. Note that the data in the contents file may be compressed (for saving storage) or encrypted (for security).

[0059] From FIGS. 5 and 6 it is readily observed that a digital work can be represented by its component parts as a hierarchy. The description tree for a digital work is comprised of a set of related descriptor blocks (d-blocks). The contents of each d-block are described with respect to FIG. 7. Referring to FIG. 7, a d-block 700 includes an identifier 701 which is a unique identifier for the work in the repository, a starting address 702 providing the start address of the first byte of the work, a length 703 giving the number of bytes in the work, a rights portion 704 wherein the granted usage rights and their status data are maintained, a parent pointer 705 for pointing to a parent d-block and child pointers 706 for pointing to the child d-blocks. In the currently preferred embodiment, the identifier 701 has two parts. The first part is a unique number assigned to the repository upon manufacture. The second part is a unique number assigned to the work upon creation. The rights portion 704

will contain a data structure, such as a look-up table, wherein the various information associated with a right is maintained. The information required by the respective usage rights is described in more detail below. D-blocks form a strict hierarchy. The top d-block of a work has no parent; all other d-blocks have one parent. The relationship of usage rights between parent and child d-blocks and how conflicts are resolved is described below.

[0060] A special type of d-block is a “shell” d-block. A shell d-block adds no new content beyond the content of its parts. A shell d-block is used to add rights and fee information, typically by distributors of digital works.

[0061] FIG. 8 illustrates a description tree for the digital work of FIG. 5. Referring to FIG. 8, a top d-block 820 for the digital work points to the various stories and advertisements contained therein. Here, the top d-block 820 points to d-block 821 (representing story A 510), d-block 822 (representing the advertisement 511), d-block 823 (representing story B 512) and d-block 824 (representing story C 513).

[0062] The portion of the description tree for Story A 510 is illustrated in FIG. 9. D-block 925 represents text 614, d-block 926 represents photo 615, d-block 927 represents graphics 616 by and d-block 928 represents sidebar 617.

[0063] The rights portion 704 of a descriptor block is further illustrated in FIG. 10. FIG. 10 illustrates a structure which is repeated in the rights portion 704 for each right. Referring to FIG. 10, each right will have a right code field 1001 and status information field 1002. The right code field 1001 will contain a unique code assigned to a right. The status information field 1002 will contain information relating to the state of a right and the digital work. Such information is indicated below in Table 1. The rights as stored in the rights portion 304 may typically be in numerical order based on the right code.

[0064] The approach for representing digital works by separating description data from content assumes that parts of a file are contiguous but takes no position on the actual representation of content. In particular, it is neutral to the question of whether content representation may take an object oriented approach. It would be natural to represent content as objects. In principle, it may be convenient to have content objects that include the billing structure and rights information that is represented in the d-blocks. Such variations in the design of the representation are possible and are viable alternatives but may introduce processing overhead, e.g. the interpretation of the objects.

Property	Value	Use
Copies-in-Use	Number	A counter of the number of copies of a work that are in use. Incremented when another copy is used; decremented when use is completed.
Loan-Period	Time-Units	Indicator of the maximum number of time-units that a document can be loaned out
Loaner-Copy	Boolean	Indicator that the current work is a loaned out copy of an authorized digital work.
Remaining-Time	Time-Units	Indicator of the remaining time of use on a metered document right.
Document-Descr	String	A string containing various identifying information about a document. The exact format of this is not specified, but it can include information such as a publisher name, author name, ISBN number, and so on.
Revenue-Owner	RO-Descr	A handle identifying a revenue owner for a digital work. This is used for reporting usage fees.
Publication-Date	Date-Descr	The date that the digital work was published.
History-list	History-Rec	A list of events recording the repostories and dates for operations that copy, transfer, backup, or restore a digital work.

TABLE 1
DIGITAL WORK STATE INFORMATION

[0065] Digital works are stored in a repository as part of a hierarchical file system. Folders (also termed directories and sub-directories) contain the digital works as well as other folders. Digital works and folders in a folder are ordered in alphabetical order. The digital works are typed to reflect how the files are used. Usage rights can be attached to folders so that the folder itself is treated as a digital work. Access to the folder would then be handled in the same fashion as any other digital work. As will be described in more detail below, the contents of the folder are subject to their own rights. Moreover, file management rights may be attached to the folder which defines how folder contents can be managed.

ATTACHING USAGE RIGHTS TO A DIGITAL WORK

[0066] It is fundamental to the present invention that the usage rights are treated as part of the digital work. As the digital work is distributed, the scope of the granted usage rights will remain the same or may be narrowed. For example, when a digital work is transferred from a document server to a repository, the usage rights may include the right to loan a copy for a predetermined period of time (called the original rights). When the repository loans out a copy of the digital work, the usage rights in the loaner copy (called the next set of rights) could be set to prohibit any further rights to loan out the copy. The basic idea is that one cannot grant more rights than they have.

[0067] The attachment of usage rights into a digital work may occur in a variety of ways. If the usage rights will be the same for an entire digital work, they could be attached when the digital work is processed for deposit in the digital work server. In the case of a digital work having different usage rights for the various components, this can be done as the digital work is being created. An authoring tool or digital work assembling tool could be utilized which provides for an automated process of attaching the usage rights.

[0068] As will be described below, when a digital work is copied, transferred or loaned, a “next set of rights” can be specified. The “next set of rights” will be attached to the digital work as it is transported.

Resolving Conflicting Rights

[0069] Because each part of a digital work may have its own usage rights, there will be instances where the rights of a “contained part” are different from its parent or container part. As a result, conflict rules must be established to dictate when and how a right may be exercised. The hierarchical structure of a digital work facilitates the enforcement of such rules. A “strict” rule would be as follows: a right for a part in a digital work is sanctioned if and only if it is sanctioned for the part, for ancestor d-blocks containing the part and for all descendent d-blocks. By sanctioned, it is meant that (1) each of the respective parts must have the right, and (2) any conditions for exercising the right are satisfied.

[0070] It also possible to implement the present invention using a more lenient rule. In the more lenient rule, access to the part may be enabled to the descendent parts which have the right, but access is denied to the descendents which do not.

[0071] Example of applying both the strict rule and lenient is illustrated with reference to FIG. 11. Referring to FIG. 11, a root d-block 1101 has child d-blocks 1102-1105.

In this case, root d-block represents a magazine, and each of the child d-blocks 1102-1105 represent articles in the magazine. Suppose that a request is made to PRINT the digital work represented by root d-block 1101 wherein the strict rule is followed. The rights for the root d-block 1101 and child d-blocks 1102-1105 are then examined. Root d-block 1101 and child d-blocks 1102 and 1105 have been granted PRINT rights. Child d-block 1103 has not been granted PRINT rights and child d-block 1104 has PRINT rights conditioned on payment of a usage fee.

[0072] Under the strict rule the PRINT right cannot be exercised because the child d-block does not have the PRINT right. Under the lenient rule, the result would be different. The digital works represented by child d-blocks 1102 and 1105 could be printed and the digital work represented by d-block 1104 could be printed so long as the usage fee is paid. Only the digital work represented by d-block 1103 could not be printed. This same result would be accomplished under the strict rule if the requests were directed to each of the individual digital works.

[0073] The present invention supports various combinations of allowing and disallowing access. Moreover, as will be described below, the usage rights grammar permits the owner of a digital work to specify if constraints may be imposed on the work by a container part. The manner in which digital works may be sanctioned because of usage rights conflicts would be implementation specific and would depend on the nature of the digital works.

REPOSITORIES

[0074] Many of the powerful functions of repositories--such as their ability to “loan” digital works or automatically handle the commercial reuse of digital works--are possible because they are trusted systems. The systems are trusted because they are able to take responsibility for fairly and reliably carrying out the commercial transactions. That the systems can be responsible (“able to respond”) is fundamentally an issue of integrity. The integrity of repositories has three parts: physical integrity, communications integrity, and behavioral integrity.

[0075] Physical integrity refers to the integrity of the physical devices themselves. Physical integrity applies both to the repositories and to the protected digital works. Thus, the higher security classes of repositories themselves may have sensors that detect when tampering is attempted on their secure cases. In addition to protection of the repository itself,

the repository design protects access to the content of digital works. In contrast with the design of conventional magnetic and optical devices--such as floppy disks, CD-ROMs, and videotapes--repositories never allow non-trusted systems to access the works directly. A maker of generic computer systems cannot guarantee that their platform will not be used to make unauthorized copies. The manufacturer provides generic capabilities for reading and writing information, and the general nature of the functionality of the general computing device depends on it. Thus, a copy program can copy arbitrary data. This copying issue is not limited to general purpose computers. It also arises for the unauthorized duplication of entertainment "software" such as video and audio recordings by magnetic recorders. Again, the functionality of the recorders depends on their ability to copy and they have no means to check whether a copy is authorized. In contrast, repositories prevent access to the raw data by general devices and can test explicit rights and conditions before copying or otherwise granting access. Information is only accessed by protocol between trusted repositories.

[0076] Communications integrity refers to the integrity of the communications channels between repositories. Roughly speaking, communications integrity means that repositories cannot be easily fooled by "telling them lies." Integrity in this case refers to the property that repositories will only communicate with other devices that are able to present proof that they are certified repositories, and furthermore, that the repositories monitor the communications to detect "impostors" and malicious or accidental interference. Thus the security measures involving encryption, exchange of digital certificates, and nonces described below are all security measures aimed at reliable communication in a world known to contain active adversaries.

[0077] Behavioral integrity refers to the integrity in what repositories do. What repositories do is determined by the software that they execute. The integrity of the software is generally assured only by knowledge of its source. Restated, a user will trust software purchased at a reputable computer store but not trust software obtained off a random (insecure) server on a network. Behavioral integrity is maintained by requiring that repository software be certified and be distributed with proof of such certification, i.e. a digital certificate. The purpose of the certificate is to authenticate that the software has been tested by an authorized organization, which attests that the software does what it is supposed to do and that it does not compromise the behavioral integrity of a repository. If the digital certificate cannot be found in the digital work or the master repository which generated the

certificate is not known to the repository receiving the software, then the software cannot be installed.

[0078] In the description of FIG. 2, it was indicated that repositories come in various forms. All repositories provide a core set of services for the transmission of digital works. The manner in which digital works are exchanged is the basis for all transaction between repositories. The various repository types differ in the ultimate functions that they perform. Repositories may be devices themselves, or they may be incorporated into other systems. An example is the rendering repository 205 of FIG. 2.

[0079] A repository will have associated with it a repository identifier. Typically, the repository identifier would be a unique number assigned to the repository at the time of manufacture. Each repository will also be classified as being in a particular security class. Certain communications and transactions may be conditioned on a repository being in a particular security class. The various security classes are described in greater detail below.

[0080] As a prerequisite to operation, a repository will require possession of an identification certificate. Identification certificates are encrypted to prevent forgery and are issued by a Master repository. A master repository plays the role of an authorization agent to enable repositories to receive digital works. Identification certificates must be updated on a periodic basis. Identification certificates are described in greater detail below with respect to the registration transaction.

[0081] A repository has both a hardware and functional embodiment. The functional embodiment is typically software executing on the hardware embodiment. Alternatively, the functional embodiment may be embedded in the hardware embodiment such as an Application Specific Integrated Circuit (ASIC) chip.

[0082] The hardware embodiment of a repository will be enclosed in a secure housing which if compromised, may cause the repository to be disabled. The basic components of the hardware embodiment of a repository are described with reference to FIG. 12. Referring to FIG. 12, a repository is comprised of a processing means 1200, storage system 1207, clock 1205 and external interface 1206. The processing means 1200 is comprised of a processor element 1201 and processor memory 1202. The processing means 1201 provides controller, repository transaction and usage rights transaction functions for the repository. Various functions in the operation of the repository such as decryption and/or decompression of digital works and transaction messages are also performed by the processing means 1200.

The processor element 1201 may be a microprocessor or other suitable computing component. The processor memory 1202 would typically be further comprised of Read Only Memories (ROM) and Random Access Memories (RAM). Such memories would contain the software instructions utilized by the processor element 1201 in performing the functions of the repository.

[0083] The storage system 1207 is further comprised of descriptor storage 1203 and content storage 1204. The description tree storage 1203 will store the description tree for the digital work and the content storage will store the associated content. The description tree storage 1203 and content storage 1204 need not be of the same type of storage medium, nor are they necessarily on the same physical device. So for example, the descriptor storage 1203 may be stored on a solid state storage (for rapid retrieval of the description tree information), while the content storage 1204 may be on a high capacity storage such as an optical disk.

[0084] The clock 1205 is used to time-stamp various time based conditions for usage rights or for metering usage fees which may be associated with the digital works. The clock 1205 will have an uninterruptible power supply, e.g. a battery, in order to maintain the integrity of the time-stamps. The external interface means 1206 provides for the signal connection to other repositories and to a credit server. The external interface means 1206 provides for the exchange of signals via such standard interfaces such as RS-232 or Personal Computer Manufacturers Card Industry Association (PCMCIA) standards, or FDDI. The external interface means 1206 may also provide network connectivity.

[0085] The functional embodiment of a repository is described with reference to FIG. 13. Referring to FIG. 13, the functional embodiment is comprised of an operating system 1301, core repository services 1302, usage transaction handlers 1303, repository specific functions, 1304 and a user interface 1305. The operating system 1301 is specific to the repository and would typically depend on the type of processor being used. The operating system 1301 would also provide the basic services for controlling and interfacing between the basic components of the repository.

[0086] The core repository services 1302 comprise a set of functions required by each and every repository. The core repository services 1302 include the session initiation transactions which are defined in greater detail below. This set of services also includes a generic ticket agent which is used to “punch” a digital ticket and a generic authorization server for processing authorization specifications. Digital tickets and authorizations are

specific mechanisms for controlling the distribution and use of digital works and are described in more detail below. Note that coupled to the core repository services are a plurality of identification certificates 1306. The identification certificates 1306 are required to enable the use of the repository.

[0087] The usage transactions handler 1303 comprise functionality for processing access requests to digital works and for billing fees based on access. The usage transactions supported will be different for each repository type. For example, it may not be necessary for some repositories to handle access requests for digital works.

[0088] The repository specific functionality 1304 comprises functionality that is unique to a repository. For example, the master repository has special functionality for issuing digital certificates and maintaining encryption keys. The repository specific functionality 1304 would include the user interface implementation for the repository.

Repository Security Classes

[0089] For some digital works the losses caused by any individual instance of unauthorized copying is insignificant and the chief economic concern lies in assuring the convenience of access and low-overhead billing. In such cases, simple and inexpensive handheld repositories and network-based workstations may be suitable repositories, even though the measures and guarantees of security are modest.

[0090] At the other extreme, some digital works such as a digital copy of a first run movie or a bearer bond or stock certificate would be of very high value so that it is prudent to employ caution and fairly elaborate security measures to ensure that they are not copied or forged. A repository suitable for holding such a digital work could have elaborate measures for ensuring physical integrity and for verifying authorization before use.

[0091] By arranging a universal protocol, all kinds of repositories can communicate with each other in principle. However, creators of some works will want to specify that their works will only be transferred to repositories whose level of security is high enough. For this reason, document repositories have a ranking system for classes and levels of security. The security classes in the currently preferred embodiment are described in Table 2.

Level	Description of Security
0	Open system. Document transmission is unencrypted. No digital certificate is required for identification. The security of the system depends mostly on user honesty, since only modest knowledge may be needed to circumvent the security measures. The repository has no provisions for preventing unauthorized programs from running and accessing or copying files. The system does not prevent the use of removable storage and does not encrypt stored files.
1	Minimal security. Like the previous class except that stored files are minimally encrypted, including ones on removable storage.
2	Basic security. Like the previous class except that special tools and knowledge are required to compromise the programming, the contents of the repository, or the state of the clock. All digital communications are encrypted. A digital certificate is provided as identification. Medium level encryption is used. Repository identification number is unforgeable.
3	General security. Like the previous class plus the requirement of special tools are needed to compromise the physical integrity of the repository and that modest encryption is used on all transmissions. Password protection is required to use the local user interface. The digital clock system cannot be reset without authorization. No works would be stored on removable storage. When executing works as programs, it runs them in their own address space and does not give them direct access to any file storage or other memory containing system code or works. They can access works only through the transmission transaction protocol.
4	Like the previous class except that high level encryption is used on all communications. Sensors are used to record attempts at physical and electronic tampering. After such tampering, the repository will not perform other transactions until it has reported such tampering to a designated server.
5	Like the previous class except that if the physical or digital attempts at tampering exceed some preset thresholds that threaten the physical integrity of the repository or the integrity of digital and cryptographic barriers, then the repository will save only document description records of history but will erase or destroy any digital identifiers that could be misused if released to an unscrupulous party. It also modifies any certificates of authenticity to indicate that the physical system has been compromised. It also erases the contents of designated documents.

TABLE 2
REPOSITORY SECURITY LEVELS

Level	Description of Security
6	Like the previous class except that the repository will attempt wireless communication to report tampering and will employ noisy alarms.
10	This would correspond to a very high level of security. This server would maintain constant communications to remote security systems reporting transactions, sensor readings, and attempts to circumvent security.

TABLE 2
REPOSITORY SECURITY LEVELS

[0092] The characterization of security levels described in Table 2 is not intended to be fixed. More important is the idea of having different security levels for different repositories. It is anticipated that new security classes and requirements will evolve according to social situations and changes in technology.

Repository User Interface

[0093] A user interface is broadly defined as the mechanism by which a user interacts with a repository in order to invoke transactions to gain access to a digital work, or exercise usage rights. As described above, a repository may be embodied in various forms. The user interface for a repository will differ depending on the particular embodiment. The user interface may be a graphical user interface having icons representing the digital works and the various transactions that may be performed. The user interface may be a generated dialog in which a user is prompted for information.

[0094] The user interface itself need not be part of the repository. As a repository may be embedded in some other device, the user interface may merely be a part of the device in which the repository is embedded. For example, the repository could be embedded in a "card" that is inserted into an available slot in a computer system. The user interface may be combination of a display, keyboard, cursor control device and software executing on the computer system.

[0095] At a minimum, the user interface must permit a user to input information such as access requests and alpha numeric data and provide feedback as to transaction status. The user interface will then cause the repository to initiate the suitable transactions to service the request. Other facets of a particular user interface will depend on the functionality that a repository will provide.

CREDIT SERVERS

[0096] In the present invention, fees may be associated with the exercise of a right. The requirement for payment of fees is described with each version of a usage right in the usage rights language. The recording and reporting of such fees is performed by the credit server. One of the capabilities enabled by associating fees with rights is the possibility of supporting a wide range of charging models. The simplest model, used by conventional software, is that there is a single fee at the time of purchase, after which the purchaser obtains unlimited rights to use the work as often and for as long as he or she wants. Alternative models, include metered use and variable fees. A single work can have different fees for different uses. For example, viewing a photograph on a display could have different fees than making a hardcopy or including it in a newly created work. A key to these alternative charging models is to have a low overhead means of establishing fees and accounting for credit on these transactions.

[0097] A credit server is a computational system that reliably authorizes and records these transactions so that fees are billed and paid. The credit server reports fees to a billing clearinghouse. The billing clearinghouse manages the financial transactions as they occur. As a result, bills may be generated and accounts reconciled. Preferably, the credit server would store the fee transactions and periodically communicate via a network with billing clearinghouse for reconciliation. In such an embodiment, communications with the billing clearinghouse would be encrypted for integrity and security reasons. In another embodiment, the credit server acts as a “debit card” where transactions occur in “real-time” against a user account.

[0098] A credit server is comprised of memory, a processing means, a clock, and interface means for coupling to a repository and a financial institution (e.g. a modem). The credit server will also need to have security and authentication functionality. These elements are essentially the same elements as those of a repository. Thus, a single device can be both a repository and a credit server, provided that it has the appropriate processing elements for carrying out the corresponding functions and protocols. Typically, however, a credit server would be a card-sized system in the possession of the owner of the credit. The credit server is coupled to a repository and would interact via financial transactions as described below. Interactions with a financial institution may occur via protocols established by the financial institutions themselves.

[0099] In the currently preferred embodiment credit servers associated with both the server and the repository report the financial transaction to the billing clearinghouse. For example, when a digital work is copied by one repository to another for a fee, credit servers coupled to each of the repositories will report the transaction to the billing clearinghouse. This is desirable in that it insures that a transaction will be accounted for in the event of some break in the communication between a credit server and the billing clearinghouse. However, some implementations may embody only a single credit server reporting the transaction to minimize transaction processing at the risk of losing some transactions.

USAGE RIGHTS LANGUAGE

[00100] The present invention uses statements in a high level “usage rights language” to define rights associated with digital works and their parts. Usage rights statements are interpreted by repositories and are used to determine what transactions can be successfully carried out for a digital work and also to determine parameters for those transactions. For example, sentences in the language determine whether a given digital work can be copied, when and how it can be used, and what fees (if any) are to be charged for that use. Once the usage rights statements are generated, they are encoded in a suitable form for accessing during the processing of transactions.

[00101] Defining usage rights in terms of a language in combination with the hierarchical representation of a digital work enables the support of a wide variety of distribution and fee schemes. An example is the ability to attach multiple versions of a right to a work. So a creator may attach a PRINT right to make 5 copies for \$10.00 and a PRINT right to make unlimited copies for \$100.00. A purchaser may then choose which option best fits his needs. Another example is that rights and fees are additive. So in the case of a composite work, the rights and fees of each of the components works is used in determining the rights and fees for the work as a whole. Other features and benefits of the usage rights language will become apparent in the description of distribution and use scenarios provided below.

[00102] The basic contents of a right are illustrated in FIG. 14. Referring to FIG. 14, a right 1450 has a transactional component 1451 and a specifications component 1452. A right 1450 has a label (e.g. COPY or PRINT) which indicate the use or distribution privileges that are embodied by the right. The transactional component 1451 corresponds to a particular way in which a digital work may be used or distributed. The transactional component 1451 is typically embodied in software instructions in a repository which implement the use or

distribution privileges for the right. The specifications components 1452 are used to specify conditions which must be satisfied prior to the right being exercised or to designate various transaction related parameters. In the currently preferred embodiment, these specifications include copy count 1453, Fees and Incentives 1454, Time 1455, Access and Security 1456 and Control 1457. Each of these specifications will be described in greater detail below with respect to the language grammar elements.

[00103] The usage rights language is based on the grammar described below. A grammar is a convenient means for defining valid sequence of symbols for a language. In describing the grammar the notation “[a | b | c]” is used to indicate distinct choices among alternatives. In this example, a sentence can have either an “a”, “b” or “c”. It must include exactly one of them. The braces { } are used to indicate optional items. Note that brackets, bars and braces are used to describe the language of usage rights sentences but do not appear in actual sentences in the language.

[00104] In contrast, parentheses are part of the usage rights language. Parentheses are used to group items together in lists. The notation (x*) is used to indicate a variable length list, that is, a list containing one or more items of type x. The notation (x)* is used to indicate a variable number of lists containing x.

[00105] Keywords in the grammar are words followed by colons. Keywords are a common and very special case in the language. They are often used to indicate a single value, typically an identifier. In many cases, the keyword and the parameter are entirely optional. When a keyword is given, it often takes a single identifier as its value. In some cases, the keyword takes a list of identifiers.

[00106] In the usage rights language, time is specified in an hours:minutes:seconds (or hh:mm:ss) representation. Time zone indicators, e.g. PDT for Pacific Daylight Time, may also be specified. Dates are represented as year/month/day (or YYYY/MMM/DD). Note that these time and date representations may specify moments in time or units of time Money units are specified in terms of dollars.

[00107] Finally, in the usage rights language, various “things” will need to interact with each other. For example, an instance of a usage right may specify a bank account, a digital ticket, etc. Such things need to be identified and are specified herein using the suffix “-ID.”

[00108] The Usage Rights Grammar is listed in its entirety in FIG. 15 and is described below.

[00109] Grammar element 1501 “Digital Work Rights:=(Rights*)” define the digital work rights as a set of rights. The set of rights attached to a digital work define how that digital work may be transferred, used, performed or played. A set of rights will attach to the entire digital work and in the case of compound digital works, each of the components of the digital work. The usage rights of components of a digital may be different.

[00110] Grammar element 1502 “Right:=(Right-Code {Copy-Count} {Control-Spec} {Time-Spec} {Access-Spec} {Fee-Spec})” enumerates the content of a right. Each usage right must specify a right code. Each right may also optionally specify conditions which must be satisfied before the right can be exercised. These conditions are copy count, control, time, access and fee conditions. In the currently preferred embodiment, for the optional elements, the following defaults apply: copy count equals 1, no time limit on the use of the right, no access tests or a security level required to use the right and no fee is required. These conditions will each be described in greater detail below.

[00111] It is important to note that a digital work may have multiple versions of a right, each having the same right code. The multiple versions would provide alternative conditions and fees for accessing the digital work.

[00112] A Grammar element 1503 “Right-Code:=Render-Code | Transport-- Code | File-Management-Code | Derivative-Works- Code Configuration-Code” distinguishes each of the specific rights into a particular right type (although each right is identified by distinct right codes). In this way, the grammar provides a catalog of possible rights that can be associated with parts of digital works. In the following, rights are divided into categories for convenience in describing them.

[00113] Grammar element 1504 “Render-Code:=[Play: {Player: Player-ID} | Print: {Printer: Printer-ID}]” lists a category of rights all involving the making of ephemeral, transitory, or non-digital copies of the digital work. After use the copies are erased.

- Play: A process of rendering or performing a digital work on some processor. This includes such things as playing digital movies, playing digital music, playing a video game, running a computer program, or displaying a document on a display.

- Print: To render the work in a medium that is not further protected by usage rights, such as printing on paper.

[00114] Grammar element 1505 “Transport-Code:=[Copy | Transfer | Loan {Remaining-Rights: Next-Set-of-Rights}]{(Next-Copy-Rights: Next-Set of Rights)}” lists a category of rights involving the making of persistent, usable copies of the digital work on other repositories. The optional Next-Copy-Rights determine the rights on the work after it is transported. If this is not specified, then the rights on the transported copy are the same as on the original. The optional Remaining-Rights specify the rights that remain with a digital work when it is loaned out. If this is not specified, then the default is that no rights can be exercised when it is loaned out.

- Copy: Make a new copy of a work
- Transfer: Moving a work from one repository to another.
- Loan: Temporarily loaning a copy to another repository for a specified period of time.

[00115] Grammar element 1506 “File-Management-Code:=Backup {Back-Up-Copy-Rights: Next-Set -of Rights} | Restore | Delete | Folder | Directory {Name:Hide-Local | Hide-Remote} {Parts:Hide-Local | Hide-Remote}” lists a category of rights involving operations for file management, such as the making of backup copies to protect the copy owner against catastrophic equipment failure.

[00116] Many software licenses and also copyright law give a copy owner the right to make backup copies to protect against catastrophic failure of equipment. However, the making of uncontrolled backup copies is inherently at odds with the ability to control usage, since an uncontrolled backup copy can be kept and then restored even after the authorized copy was sold.

[00117] The File management rights enable the making and restoring of backup copies in a way that respects usage rights, honoring the requirements of both the copy owner and the rights grantor and revenue owner. Backup copies of work descriptions (including usage rights and fee data) can be sent under appropriate protocol and usage rights control to other document repositories of sufficiently high security. Further rights permit organization of digital works into folders which themselves are treated as digital works and whose contents may be “hidden” from a party seeking to determine the contents of a repository.

- Backup: To make a backup copy of a digital work as protection against media failure.
- Restore: To restore a backup copy of a digital work.

- Delete: To delete or erase a copy of a digital work.
- Folder: To create and name folders, and to move files and folders between folders.
- Directory: To hide a folder or it's contents.

[00118] Grammar element 1507 “Derivative-Works-Code: [Extract | Embed | Edit {Process: Process-ID}] {Next-Copy-Rights: Next-Set-of Rights}” lists a category of rights involving the use of a digital work to create new works.

- Extract: To remove a portion of a work, for the purposes of creating a new work.
- Embed: To include a work in an existing work.
- Edit: To alter a digital work by copying, selecting and modifying portions of an existing digital work.

[00119] Grammar element 1508 “Configuration-Code:=Install | Uninstall” lists a category of rights for installing and uninstalling software on a repository (typically a rendering repository.) This would typically occur for the installation of a new type of player within the rendering repository.

- Install: To install new software on a repository.
- Uninstall: To remove existing software from a repository.

[00120] Grammar element 1509 “Next-Set-of-Rights:={ (Add: Set-Of-Rights)} {(Delete: Set-Of-Rights)} {(Replace: Set-Of-Rights)} {(Keep: Set-Of-Rights)}” defines how rights are carried forward for a copy of a digital work. If the Next-Copy-Rights is not specified, the rights for the next copy are the same as those of the current copy. Otherwise, the set of rights for the next copy can be specified. Versions of rights after Add: are added to the current set of rights. Rights after Delete: are deleted from the current set of rights. If only right codes are listed after Delete:, then all versions of rights with those codes are deleted. Versions of rights after Replace: subsume all versions of rights of the same type in the current set of rights.

[00121] If Remaining-Rights is not specified, then there are no rights for the original after all Loan copies are loaned out. If Remaining-Rights is specified, then the Keep: token can be used to simplify the expression of what rights to keep behind. A list of right codes following keep means that all of the versions of those listed rights are kept in the remaining copy. This specification can be overridden by subsequent Delete: or Replace: specifications.

Copy Count Specification

[00122] For various transactions, it may be desirable to provide some limit as to the number of “copies” of the work which may be exercised simultaneously for the right. For example, it may be desirable to limit the number of copies of a digital work that may be loaned out at a time or viewed at a time.

[00123] Grammar element 1510 “Copy-Count:=(Copies: positive-integer | 0 | unlimited)” provides a condition which defines the number of “copies” of a work subject to the right. A copy count can be 0, a fixed number, or unlimited. The copy-count is associated with each right, as opposed to there being just a single copy-count for the digital work. The Copy-Count for a right is decremented each time that a right is exercised. When the Copy-Count equals zero, the right can no longer be exercised. If the Copy-Count is not specified, the default is one.

Control Specification

[00124] Rights and fees depend in general on rights granted by the creator as well as further restrictions imposed by later distributors. Control specifications deal with interactions between the creators and their distributors governing the imposition of further restrictions and fees. For example, a distributor of a digital work may not want an end consumer of a digital work to add fees or otherwise profit by commercially exploiting the purchased digital work.

[00125] Grammar element 1511 “Control-Spec:=(Control: {Restrictable | Unrestrictable} {Unchargeable | Chargeable}-)” provides a condition to specify the effect of usage rights and fees of parents on the exercise of the right. A digital work is restrictable if higher level d-blocks can impose further restrictions (time specifications and access specifications) on the right. It is unrestrictable if no further restrictions can be imposed. The default setting is restrictable. A right is unchargeable if no more fees can be imposed on the use of the right. It is chargeable if more fees can be imposed. The default is chargeable.

Time Specification

[00126] It is often desirable to assign a start date or specify some duration as to when a right may be exercised. Grammar element 1512 “Time-Spec:=({Fixed-Interval | Sliding-Interval | Meter-Tim- e} Until: Expiration-Date)” provides for specification of time conditions on the exercise of a right. Rights may be granted for a specified time. Different kinds of time specifications are appropriate for different kinds of rights. Some rights may be exercised during a fixed and predetermined duration. Some rights may be exercised for an interval that starts the first time that the right is invoked by some transaction. Some rights

may be exercised or are charged according to some kind of metered time, which may be split into separate intervals. For example, a right to view a picture for an hour might be split into six ten minute viewings or four fifteen minute viewings or twenty three minute viewings.

[00127] The terms “time” and “date” are used synonymously to refer to a moment in time. There are several kinds of time specifications. Each specification represents some limitation on the times over which the usage right applies. The Expiration-Date specifies the moment at which the usage right ends. For example, if the Expiration-Date is “Jan. 1, 1995,” then the right ends at the first moment of 1995. If the Expiration-Date is specified as *forever*, then the rights are interpreted as continuing without end. If only an expiration date is given, then the right can be exercised as often as desired until the expiration date.

[00128] Grammar element 1513 “Fixed-Interval:=From: Start-Time” is used to define a predetermined interval that runs from the start time to the expiration date.

[00129] Grammar element 1514 “Sliding-Interval:=Interval: Use-Duration” is used to define an indeterminate (or “open”) start time. It sets limits on a continuous period of time over which the contents are accessible. The period starts on the first access and ends after the duration has passed or the expiration date is reached, whichever comes first. For example, if the right gives 10 hours of continuous access, the use-duration would begin when the first access was made and end 10 hours later.

[00130] Grammar element 1515 “Meter-Time:=Time-Remaining: Remaining-Use” is used to define a “meter time,” that is, a measure of the time that the right is actually exercised. It differs from the Sliding-Interval specification in that the time that the digital work is in use need not be continuous. For example, if the rights guarantee three days of access, those days could be spread out over a month. With this specification, the rights can be exercised until the meter time is exhausted or the expiration date is reached, whichever comes first.

Remaining-Use:=Time-Unit

Start-Time:=Time-Unit

Use-Duration:=Time-Unit

[00131] All of the time specifications include time-unit specifications in their ultimate instantiation.

Security Class and Authorization Specification

[00132] The present invention provides for various security mechanisms to be introduced into a distribution or use scheme. Grammar element 1516 “Access-Spec=(`{SC: Security-Class} {Authorization: Authorization-ID*} {Other-Authorization: Authorization-ID*} {Ticket: Ticket-ID}`)” provides a means for restricting access and transmission. Access specifications can specify a required security class for a repository to exercise a right or a required authorization test that must be satisfied.

[00133] The keyword “SC:” is used to specify a minimum security level for the repositories involved in the access. If “SC:” is not specified, the lowest security level is acceptable.

[00134] The optional “Authorization:” keyword is used to specify required authorizations on the same repository as the work. The optional “Other-Authorization:” keyword is used to specify required authorizations on the other repository in the transaction.

[00135] The optional “Ticket:” keyword specifies the identity of a ticket required for the transaction. A transaction involving digital tickets must locate an appropriate digital ticket agent who can “punch” or otherwise validate the ticket before the transaction can proceed. Tickets are described in greater detail below.

[00136] In a transaction involving a repository and a document server, some usage rights may require that the repository have a particular authorization, that the server have some authorization, or that both repositories have (possibly different) authorizations. Authorizations themselves are digital works (hereinafter referred to as an authorization object) that can be moved between repositories in the same manner as other digital works. Their copying and transferring is subject to the same rights and fees as other digital works. A repository is said to have an authorization if that authorization object is contained within the repository.

[00137] In some cases, an authorization may be required from a source other than the document server and repository. An authorization object referenced by an Authorization-ID can contain digital address information to be used to set up a communications link between a repository and the authorization source. These are analogous to phone numbers. For such access tests, the communication would need to be established and authorization obtained before the right could be exercised.

[00138] For one-time usage rights, a variant on this scheme is to have a digital ticket. A ticket is presented to a digital ticket agent, whose type is specified on the ticket. In the

simplest case, a certified generic ticket agent, available on all repositories, is available to “punch” the ticket. In other cases, the ticket may contain addressing information for locating a “special” ticket agent. Once a ticket has been punched, it cannot be used again for the same kind of transaction (unless it is unpunched or refreshed in the manner described below.) Punching includes marking the ticket with a timestamp of the date and time it was used. Tickets are digital works and can be copied or transferred between repositories according to their usage rights.

[00139] In the currently preferred embodiment, a “punched” ticket becomes “unpunched” or “refreshed” when it is copied or extracted. The Copy and Extract operations save the date and time as a property of the digital ticket. When a ticket agent is given a ticket, it can simply check whether the digital copy was made after the last time that it was punched. Of course, the digital ticket must have the copy or extract usage rights attached thereto.

[00140] The capability to unpunch a ticket is important in the following cases:

- A digital work is circulated at low cost with a limitation that it can be used only once.
- A digital work is circulated with a ticket that can be used once to give discounts on purchases of other works.
- A digital work is circulated with a ticket (included in the purchase price and possibly embedded in the work) that can be used for a future upgrade.

[00141] In each of these cases, if a paid copy is made of the digital work (including the ticket) the new owner would expect to get a fresh (unpunched) ticket, whether the copy seller has used the work or not. In contrast, loaning a work or simply transferring it to another repository should not revitalize the ticket.

Usage Fees and Incentives Specification

[00142] The billing for use of a digital work is fundamental to a commercial distribution system. Grammar Element 1517 “Fee-Spec:={Scheduled-Discount} Regular-Fee-Spec | Scheduled-Fee-Spec | Markup-Spec” provides a range of options for billing for the use of digital works.

[00143] A key feature of this approach is the development of low-overhead billing for transactions in potentially small amounts. Thus, it becomes feasible to collect fees of only a few cents each for thousands of transactions.

[00144] The grammar differentiates between uses where the charge is per use from those where it is metered by the time unit. Transactions can support fees that the user pays for using a digital work as well as incentives paid by the right grantor to users to induce them to use or distribute the digital work.

[00145] The optional scheduled discount refers to the rest of the fee specification--discounting it by a percentage over time. If it is not specified, then there is no scheduled discount. Regular fee specifications are constant over time. Scheduled fee specifications give a schedule of dates over which the fee specifications change. Markup specifications are used in d-blocks for adding a percentage to the fees already being charged.

[00146] Grammar Element 1518 “Scheduled-Discount:=(Scheduled-Discount: (Time-Spec Percentage*))” A Scheduled-Discount is essentially a scheduled modifier of any other fee specification for this version of the right of the digital work. (It does not refer to children or parent digital works or to other versions of rights.). It is a list of pairs of times and percentages. The most recent time in the list that has not yet passed at the time of the transaction is the one in effect. The percentage gives the discount percentage. For example, the number 10 refers to a 10% discount.

[00147] Grammar Element 1519 “Regular-Fee-Spec:=({Fee: | Incentive:} [Per-Use-Spec | Metered-Rate-Spec | Best-Price-Spec | Call-For-Price-Spec] {Min: Money-Unit Per: Time-Spec} {Max: Money-Unit Per: Time-Spec} To: Account-ID)” provides for several kinds of fee specifications.

[00148] Fees are paid by the copy-owner/user to the revenue-owner if Fee: is specified. Incentives are paid by the revenue-owner to the user if Incentive: is specified. If the Min: specification is given, then there is a minimum fee to be charged per time-spec unit for its use. If the Max: specification is given, then there is a maximum fee to be charged per time-spec for its use. When Fee: is specified, Account-ID identifies the account to which the fee is to be paid. When Incentive: is specified, Account-ID identifies the account from which the fee is to be paid.

[00149] Grammar element 1520 “Per-Use-Spec:=Per-Use: Money-unit” defines a simple fee to be paid every time the right is exercised, regardless of how much time the transaction takes.

[00150] Grammar element 1521 “Metered-Rate-Spec:=Metered: Money-Unit Per: Time-Spec” defines a metered-rate fee paid according to how long the right is exercised. Thus, the time it takes to complete the transaction determines the fee.

[00151] Grammar, element 1522 “Best-Price-Spec:=Best-Price: Money-unit Max: Money-unit” is used to specify a best-price that is determined when the account is settled. This specification is to accommodate special deals, rebates, and pricing that depends on information that is not available to the repository. All fee specifications can be combined with tickets or authorizations that could indicate that the consumer is a wholesaler or that he is a preferred customer, or that the seller be authorized in some way. The amount of money in the Max: field is the maximum amount that the use will cost. This is the amount that is tentatively debited from the credit server. However, when the transaction is ultimately reconciled, any excess amount will be returned to the consumer in a separate transaction.

[00152] Grammar element 1523 “Call-For-Price-Spec:=Call-For-Price “ is similar to a “Best-Price-Spec” in that it is intended to accommodate cases where prices are dynamic. A Call-For-Price Spec requires a communication with a dealer to determine the price. This option cannot be exercised if the repository cannot communicate with a dealer at the time that the right is exercised. It is based on a secure transaction whereby the dealer names a price to exercise the right and passes along a deal certificate which is referenced or included in the billing process.

[00153] Grammar element 1524 “Scheduled-Fee-Spec:=(Schedule: (Time-Spec Regular-Fee-Spec)*)” is used to provide a schedule of dates over which the fee specifications change. The fee specification with the most recent date not in the future is the one that is in effect. This is similar to but more general than the scheduled discount. It is more general, because it provides a means to vary the fee agreement for each time period.

[00154] Grammar element 1525 “Markup-Spec:=Markup: percentage To: Account-ID” is provided for adding a percentage to the fees already being charged. For example, a 5% markup means that a fee of 5% of cumulative fee so far will be allocated to the distributor. A markup specification can be applied to all of the other kinds of fee specifications. It is typically used in a shell provided by a distributor. It refers to fees associated with d-blocks that are parts of the current d-block. This might be a convenient specification for use in taxes, or in distributor overhead.

Examples of Sets of Usage Rights

- ((Play) (Transfer (SC: 3)) (Delete)

[00155] This work can be played without requirements for fee or authorization on any rendering system. It can be transferred to any other repository of security level 3 or greater. It can be deleted.

- ((Play) (Transfer (SC: 3)) (Delete) (Backup) (Restore (Fee:Per-Use: \$5 To: Account-ID-678))))

[00156] Same as the previous example plus rights for backup and restore. The work can be backed up without fee. It can be restored for a \$5 fee payable to the account described by Account-ID-678.

- ((Play) (Transfer (SC: 3))
(Copy (SC:3)(Fee: Per-Use: \$5 To: Account-ID-678))
(Delete (Incentive: Per-Use: \$2.50 To: Account-ID-678))))

[00157] This work can be played, transferred, copied, or deleted. Copy or transfer operations can take place only with repositories of security level three or greater. The fee to make a copy is \$5 payable to Account-ID-678. If a copy is deleted, then an incentive of \$2.50 is paid to the former copy owner.

- ((Play) (Transfer (SC: 3))
Copy (SC: 3) (Fee: Per-Use: \$10 To: Account-ID-678))
Delete) (Backup) (Restore (SC: 3) (Fee: Per-Use: \$5 To: Account-ID-678))))

[00158] Same as the previous example plus fees for copying. The work can be copied digitally for a fee of \$10 payable to Account-ID-678. The repository on which the work is copied or restored must be at security level 3 or greater.

- ((Play) (Transfer (SC: 3))
(Copy Authorization: License-123-ID (SC: 3))))

[00159] The digital work can be played, transferred, or copied. Copies or transfers must be on repositories of security level 3 or greater. Copying requires the license License-123-ID issued to the copying repository. None of the rights require fees.

- ((Play) (Print Printer: Printer-567-ID (Fee: Per-Use: \$1 To: Account-ID-678))))

[00160] This work can be played for free. It can be printed on any printer with the identifier Printer-567-ID for a fee of \$1 payable to the account described by Account-ID-678.

- ((Play Player: Player-876-ID) (From: Feb. 2, 1994 Until: Feb. 15, 1995) (Fee: Metered: \$0.01 Per: 0:1:0 Min: \$0.25 Per: 0/1/0 To: Account-ID-567))

[00161] This work can be played on any player holding the ID Player-876-ID. The time of this right is from Feb. 14, 1994 until Feb. 15, 1995. The fee for use is one cent per minute with a minimum of 25 cents in any day that it is used, payable to the account described by Account-ID-567.

- ((Play) (Transfer) (Delete)(Loan 2 (Delete: Transfer Loan)))

[00162] This work can be played, transferred, deleted, or loaned. Up to two copies can be loaned out at a time. The loaned copy has the same rights except that it cannot be transferred. When both copies are loaned out, no rights can be exercised on the original on the repository.

[00163] • ((Play) (Transfer) (Delete) (Backup) (Restore (SC:3))

(Loan 2 Remaining-Copy-Rights: (Delete: Play Transfer)

Next-Set-of-Rights: (Delete: Transfer Loan)))

[00164] Similar to previous example. Rights to Backup and Restore the work are added, where restoration requires a repository of at least security level three. When all copies of the work are loaned out, the remaining copy cannot be played or transferred.

- ((Play) (Transfer) (Copy) (Print) (Backup) (Restore (SC:3))

(Loan 1 Remaining-Copy-Rights: (Add: Play Print Backup)

Next-Set-of-Rights: (Delete: Transfer Loan)

(Fee: Metered: \$10 Per: 1:0:0 To: Account-ID-567))

(Loan 1 Remaining-Copy-Rights:

Add: ((Play Player: Player-876-ID) 2 (From: Feb. 14, 1994 Until: Feb. 15, 1995)

(Fee: Metered: \$0.01 Per: 0:1:0 Min: \$0.25 Per: 0/1/0

To: Account-ID-567))))

[00165] The original work has rights to Play, Transfer, Copy, Print, Backup, Restore, and Loan. There are two versions of the Loan right. The first version of the loan right costs \$10 per day but allows the original copy owner to exercise free use of the Play, Print and Backup rights. The second version of the Loan right is free. None of the original rights are applicable. However a right to Play the work at the specified metered rate is added.

- ((Play Player: Player-Small-Screen-123-ID)

(Embed (Fee: Per-Use \$0.01 To: Account-678-ID))

(Copy (Fee: Per-Use \$1.00 To: Account-678-ID)))

[00166] The digital work can be played on any player with the identifier Player-Small-Screen-123-ID. It can be embedded in a larger work. The embedding requires a modest one cent registration fee to Account-678-ID. Digital copies can be made for \$1.00.

REPOSITORY TRANSACTIONS

[00167] When a user requests access to a digital work, the repository will initiate various transactions. The combination of transactions invoked will depend on the specifications assigned for a usage right. There are three basic types of transactions, Session Initiation Transactions, Financial Transactions and Usage Transactions. Generally, session initiation transactions are initiated first to establish a valid session. When a valid session is established, transactions corresponding to the various usage rights are invoked. Finally, request specific transactions are performed.

[00168] Transactions occur between two repositories (one acting as a server), between a repository and a document playback platform (e.g. for executing or viewing), between a repository and a credit server or between a repository and an authorization server. When transactions occur between more than one repository, it is assumed that there is a reliable communication channel between the repositories. For example, this could be a TCP/IP channel or any other commercially available channel that has built-in capabilities for detecting and correcting transmission errors. However, it is not assumed that the communication channel is secure. Provisions for security and privacy are part of the requirements for specifying and implementing repositories and thus form the need for various transactions.

Message Transmission

[00169] Transactions require that there be some communication between repositories. Communication between repositories occurs in units termed as messages. Because the communication line is assumed to be unsecure, all communications with repositories that are above the lowest security class are encrypted utilizing a public key encryption technique. Public key encryption is a well known technique in the encryption arts. The term key refers to a numeric code that is used with encryption and decryption algorithms. Keys come in pairs, where “writing keys” are used to encrypt data and “checking keys” are used to decrypt data. Both writing and checking keys may be public or private. Public keys are those that are distributed to others. Private keys are maintained in confidence.

[00170] Key management and security is instrumental in the success of a public key encryption system. In the currently preferred embodiment, one or more master repositories maintain the keys and create the identification certificates used by the repositories.

[00171] When a sending repository transmits a message to a receiving repository, the sending repository encrypts all of its data using the public writing key of the receiving repository. The sending repository includes its name, the name of the receiving repository, a session identifier such as a nonce (described below), and a message counter in each message.

[00172] In this way, the communication can only be read (to a high probability) by the receiving repository, which holds the private checking key for decryption. The auxiliary data is used to guard against various replay attacks to security. If messages ever arrive with the wrong counter or an old nonce, the repositories can assume that someone is interfering with communication and the transaction terminated.

[00173] The respective public keys for the repositories to be used for encryption are obtained in the registration transaction described below.

Session Initiation Transactions

[00174] A usage transaction is carried out in a session between repositories. For usage transactions involving more than one repository, or for financial transactions between a repository and a credit server, a registration transaction is performed. A second transaction termed a login transaction, may also be needed to initiate the session. The goal of the registration transaction is to establish a secure channel between two repositories who know each others identities. As it is assumed that the communication channel between the repositories is reliable but not secure, there is a risk that a non-repository may mimic the protocol in order to gain illegitimate access to a repository.

[00175] The registration transaction between two repositories is described with respect to FIGS. 16 and 17. The steps described are from the perspective of a “repository-1” registering its identity with a “repository-2”. The registration must be symmetrical so the same set of steps will be repeated for repository-2 registering its identity with repository-1. Referring to FIG. 16, repository-1 first generates an encrypted registration identifier, step 1601 and then generates a registration message, step 1602. A registration message is comprised of an identifier of a master repository, the identification certificate for the repository-1 and an encrypted random registration identifier. The identification certificate is encrypted by the master repository in its private key and attests to the fact that the repository

(here repository-1) is a bona fide repository. The identification certificate also contains a public key for the repository, the repository security level and a timestamp (indicating a time after which the certificate is no longer valid.) The registration identifier is a number generated by the repository for this registration. The registration identifier is unique to the session and is encrypted in repository-1's private key. The registration identifier is used to improve security of authentication by detecting certain kinds of communications based attacks. Repository-1 then transmits the registration message to repository-2, step 1603.

[00176] Upon receiving the registration message, repository-2 determines if it has the needed public key for the master repository, step 1604. If repository-2 does not have the needed public key to decrypt the identification certificate, the registration transaction terminates in an error, step 1618.

[00177] Assuming that repository-2 has the proper public key the identification certificate is decrypted, step 1605. Repository-2 saves the encrypted registration identifier, step 1606, and extracts the repository identifier, step 1607. The extracted repository identifier is checked against a "hotlist" of compromised document repositories, step 1608. In the currently preferred embodiment, each repository will contain "hotlists" of compromised repositories. If the repository is on the "hotlist", the registration transaction terminates in an error per step 1618. Repositories can be removed from the hotlist when their certificates expire, so that the list does not need to grow without bound. Also, by keeping a short list of hotlist certificates that it has previously received, a repository can avoid the work of actually going through the list. These lists would be encrypted by a master repository. A minor variation on the approach to improve efficiency would have the repositories first exchange lists of names of hotlist certificates, ultimately exchanging only those lists that they had not previously received. The "hotlists" are maintained and distributed by Master repositories.

[00178] Note that rather than terminating in error, the transaction could request that another registration message be sent based on an identification certificate created by another master repository. This may be repeated until a satisfactory identification certificate is found, or it is determined that trust cannot be established.

[00179] Assuming that the repository is not on the hotlist, the repository identification needs to be verified. In other words, repository-2 needs to validate that the repository on the other end is really repository-1. This is termed performance testing and is performed in order to avoid invalid access to the repository via a counterfeit repository replaying a recording of a

prior session initiation between repository-1 and repository-2. Performance testing is initiated by repository-2 generating a performance message, step 1609. The performance message consists of a nonce, the names of the respective repositories, the time and the registration identifier received from repository-1. A nonce is a generated message based on some random and variable information (e.g. the time or the temperature.) The nonce is used to check whether repository-1 can actually exhibit correct encrypting of a message using the private keys it claims to have, on a message that it has never seen before. The performance message is encrypted using the public key specified in the registration message of repository-1. The performance message is transmitted to repository-1, step 1610, where it is decrypted by repository-1 using its private key, step 1611. Repository-1 then checks to make sure that the names of the two repositories are correct, step 1612, that the time is accurate, step 1613 and that the registration identifier corresponds to the one it sent, step 1614. If any of these tests fails, the transaction is terminated per step 1616. Assuming that the tests are passed, repository-1 transmits the nonce to repository-2 in the clear, step 1615. Repository-2 then compares the received nonce to the original nonce, step 1617. If they are not identical, the registration transaction terminates in an error per step 1618. If they are the same, the registration transaction has successfully completed.

[00180] At this point, assuming that the transaction has not terminated, the repositories exchange messages containing session keys to be used in all communications during the session and synchronize their clocks. FIG. 17 illustrates the session information exchange and clock synchronization steps (again from the perspective of repository-1.) Referring to FIG. 17, repository-1 creates a session key pair, step 1701. A first key is kept private and is used by repository-1 to encrypt messages. The second key is a public key used by repository-2 to decrypt messages. The second key is encrypted using the public key of repository-2, step 1702 and is sent to repository-2, step 1703. Upon receipt, repository-2 decrypts the second key, step 1704. The second key is used to decrypt messages in subsequent communications. When each repository has completed this step, they are both convinced that the other repository is bona fide and that they are communicating with the original. Each repository has given the other a key to be used in decrypting further communications during the session. Since that key is itself transmitted in the public key of the receiving repository only it will be able to decrypt the key which is used to decrypt subsequent messages.

[00181] After the session information is exchanged, the repositories must synchronize their clocks. Clock synchronization is used by the repositories to establish an agreed upon

time base for the financial records of their mutual transactions. Referring back to FIG. 17, repository-2 initiates clock synchronization by generating a time stamp exchange message, step 1705, and transmits it to repository-1, step 1706. Upon receipt, repository-1 generates its own time stamp message, step 1707 and transmits it back to repository-2, step 1708. Repository-2 notes the current time, step 1709 and stores the time received from repository-1, step 1710. The current time is compared to the time received from repository-1, step 1711. The difference is then checked to see if it exceeds a predetermined tolerance (e.g. one minute), step 1712. If it does, repository-2 terminates the transaction as this may indicate tampering with the repository, step 1713. If not repository-2 computes an adjusted time delta, step 1714. The adjusted time delta is the difference between the clock time of repository-2 and the average of the times from repository-1 and repository-2.

[00182] To achieve greater accuracy, repository-2 can request the time again up to a fixed number of times (e.g. five times), repeat the clock synchronization steps, and average the results.

[00183] A second session initiation transaction is a Login transaction. The Login transaction is used to check the authenticity of a user requesting a transaction. A Login transaction is particularly prudent for the authorization of financial transactions that will be charged to a credit server. The Login transaction involves an interaction between the user at a user interface and the credit server associated with a repository. The information exchanged here is a login string supplied by the repository/credit server to identify itself to the user, and a Personal Identification Number (PIN) provided by the user to identify himself to the credit server. In the event that the user is accessing a credit server on a repository different from the one on which the user interface resides, exchange of the information would be encrypted using the public and private keys of the respective repositories.

Billing Transactions

[00184] Billing Transactions are concerned with monetary transaction with a credit server. Billing Transactions are carried out when all other conditions are satisfied and a usage fee is required for granting the request. For the most part, billing transactions are well understood in the state of the art. These transactions are between a repository and a credit server, or between a credit server and a billing clearinghouse. Briefly, the required transactions include the following:

- Registration and LOGIN transactions, by which the repository and user establish their bona fides to a credit server. These transactions would be entirely internal in cases where the repository and credit server are implemented as a single system.

- Registration and LOGIN transactions, by which a credit server establishes its bona fides to a billing clearinghouse.

- An Assign-fee transaction to assign a charge. The information in this transaction would include a transaction identifier, the identities of the repositories in the transaction, and a list of charges from the parts of the digital work. If there has been any unusual event in the transaction such as an interruption of communications, that information is included as well.

- A Begin-charges transaction to assign a charge. This transaction is much the same as an assign-fee transaction except that it is used for metered use. It includes the same information as the assign-fee 4, ii transaction as well as the usage fee information. The credit-server is then responsible for running a clock.

- An End-charges transaction to end a charge for metered use. (In a variation on this approach, the repositories would exchange periodic charge information for each block of time.)

- A report-charges transaction between a personal credit server and a billing clearinghouse. This transaction is invoked at least once per billing period. It is used to pass along information about charges. On debit and credit cards, this transaction would also be used to update balance information and credit limits as needed.

[00185] All billing transactions are given a transaction ID and are reported to the credit servers by both the server and the client. This reduces possible loss of billing information if one of the parties to a transaction loses a banking card and provides a check against tampering with the system.

Usage Transactions

[00186] After the session initiation transactions have been completed, the usage request may then be processed. To simplify the description of the steps carried out in processing a usage request, the term requester is used to refer to a repository in the requester mode which is initiating a request, and the term server is used to refer to a repository in the server mode and which contains the desired digital work. In many cases such as requests to print or view a work, the requester and server may be the same device and the transactions described in the following would be entirely internal. In such instances, certain transaction steps, such as the registration transaction, need not be performed.

[00187] There are some common steps that are part of the semantics of all of the usage rights transactions. These steps are referred to as the common transaction steps. There are two sets--the “opening” steps and the “closing” steps. For simplicity, these are listed here rather than repeating them in the descriptions of all of the usage rights transactions.

[00188] Transactions can refer to a part of a digital work, a complete digital work, or a Digital work containing other digital works. Although not described in detail herein, a transaction may even refer to a folder comprised of a plurality of digital works. The term “work” is used to refer to what ever portion or set of digital works is being accessed.

[00189] Many of the steps here involve determining if certain conditions are satisfied. Recall that each usage right may have one or more conditions which must be satisfied before the right can be exercised. Digital works have parts and parts have parts. Different parts can have different rights and fees. Thus, it is necessary to verify that the requirements are met for ALL of the parts that are involved in a transaction For brevity, when reference is made to checking whether the rights exist and conditions for exercising are satisfied, it is meant that all such checking takes place for each of the relevant parts of the work.

[00190] FIG. 18 illustrates the initial common opening and closing steps for a transaction. At this point it is assumed that registration has occurred and that a “trusted” session is in place. General tests are tests on usage rights associated with the folder containing the work or some containing folder higher in the file system hierarchy. These tests correspond to requirements imposed on the work as a consequence of its being on the particular repository, as opposed to being attached to the work itself. Referring to FIG. 18, prior to initiating a usage transaction, the requester performs any general tests that are required before the right associated with the transaction can be exercised, step, 1801. For example, install, uninstall and delete rights may be implemented to require that a requester have an authorization certificate before the right can be exercised. Another example is the requirement that a digital ticket be present and punched before a digital work may be copied to a requester. If any of the general tests fail, the transaction is not initiated, step, 1802. Assuming that such required tests are passed, upon receiving the usage request, the server generates a transaction identifier that is used in records or reports of the transaction, step 1803. The server then checks whether the digital work has been granted the right corresponding to the requested transaction, step 1804. If the digital work has not been granted the right corresponding to the request, the transaction terminates, step 1805. If the digital work has been granted the requested right, the server then determines if the various

conditions for exercising the right are satisfied. Time based conditions are examined, step 1806. These conditions are checked by examining the time specification for the version of the right. If any of the conditions are not satisfied, the transaction terminates per step 1805.

[00191] Assuming that the time based conditions are satisfied, the server checks security and access conditions, step 1807. Such security and access conditions are satisfied if: 1) the requester is at the specified security class, or a higher security class, 2) the server satisfies any specified authorization test and 3) the requester satisfies any specified authorization tests and has any required digital tickets. If any of the conditions are not satisfied, the transaction terminates per step 1805.

[00192] Assuming that the security and access conditions are all satisfied, the server checks the copy count condition, step 1808. If the copy count equals zero, then the transaction cannot be completed and the transaction terminates per step 1805.

[00193] Assuming that the copy count does not equal zero, the server checks if the copies in use for the requested right is greater than or equal to any copy count for the requested right (or relevant parts), step 1809. If the copies in use are greater than or equal to the copy count, this indicates that usage rights for the version of the transaction have been exhausted. Accordingly, the server terminates the transaction, step 1805. If the copy count is less than the copies in use for the transaction the transaction can continue, and the copies in use would be incremented by the number of digital works requested in the transaction, step 1810.

[00194] The server then checks if the digital work has a “Loan” access right, step 1811. The “Loan” access right is a special case since remaining rights may be present even though all copies are loaned out. If the digital work has the “Loan” access right, a check is made to see if all copies have been loaned out, step 1812. The number of copies that could be loaned is the sum of the Copy-Counts for all of the versions of the loan right of the digital work. For a composite work, the relevant figure is the minimal such sum of each of the components of the composite work. If all copies have been loaned out, the remaining rights are determined, step 1813. The remaining-rights are determined from the remaining rights specifications from the versions of the Loan right. If there is only one version of the Loan right, then the determination is simple. The remaining rights are the ones specified in that version of the Loan right, or none if Remaining-Rights: is not specified. If there are multiple versions of the Loan right and all copies of all of the versions are loaned out, then the

remaining rights is taken as the minimum set (intersection) of remaining rights across all of the versions of the loan right. The server then determines if the requested right is in the set of remaining rights, step 1814. If the requested right is not in the set of remaining rights, the server terminates the transaction, step 1805.

[00195] If Loan is not a usage right for the digital work or if all copies have not been loaned out or the requested right is in the set of remaining rights, fee conditions for the right are then checked, step 1815. This will initiate various financial transactions between the repository and associated credit server. Further, any metering of usage of a digital work will commence. If any financial transaction fails, the transaction terminates per step 1805.

[00196] It should be noted that the order in which the conditions are checked need not follow the order of steps 1806-1815.

[00197] At this point, right specific steps are now performed and are represented here as step 1816. The right specific steps are described in greater detail below.

[00198] The common closing transaction steps are now performed. Each of the closing transaction steps are performed by the server after a successful completion of a transaction. Referring back to FIG. 18, the copies in use value for the requested right is decremented by the number of copies involved in the transaction, step 1817. Next, if the right had a metered usage fee specification, the server subtracts the elapsed time from the Remaining-Use-Time associated with the right for every part involved in the transaction, step 1818. Finally, if there are fee specifications associated with the right, the server initiates End-Charge financial transaction to confirm billing, step 1819.

Transmission Protocol

[00199] An important area to consider is the transmission of the digital work from the server to the requester. The transmission protocol described herein refers to events occurring after a valid session has been created. The transmission protocol must handle the case of disruption in the communications between the repositories. It is assumed that interference such as injecting noise on the communication channel can be detected by the integrity checks (e.g., parity, checksum, etc.) that are built into the transport protocol and are not discussed in detail herein.

[00200] The underlying goal in the transmission protocol is to preclude certain failure modes, such as malicious or accidental interference on the communications channel. Suppose, for example, that a user pulls a card with the credit server at a specific time near the

end of a transaction. There should not be a vulnerable time at which “pulling the card” causes the repositories to fail to correctly account for the number of copies of the work that have been created. Restated, there should be no time at which a party can break a connection as a means to avoid payment after using a digital work.

[00201] If a transaction is interrupted (and fails), both repositories restore the digital works and accounts to their state prior to the failure, modulo records of the failure itself.

[00202] FIG. 19 is a state diagram showing steps in the process of transmitting information during a transaction. Each box represents a state of a repository in either the server mode (above the central dotted line 1901) or in the requester mode (below the dotted line 1901). Solid arrows stand for transitions between states. Dashed arrows stand for message communications between the repositories. A dashed message arrow pointing to a solid transition arrow is interpreted as meaning that the transition takes place when the message is received. Unlabeled transition arrows take place unconditionally. Other labels on state transition arrows describe conditions that trigger the transition.

[00203] Referring now to FIG. 19, the server is initially in a state 1902 where a new transaction is initiated via start message 1903. This message includes transaction information including a transaction identifier and a count of the blocks of data to be transferred. The requester, initially in a wait state 1904 then enters a data wait state 1905.

[00204] The server enters a data transmit state 1906 and transmits a block of data 1907 and then enters a wait for acknowledgement state 1908. As the data is received, the requesters enters a data receive state 1909 and when the data blocks is completely received it enters an acknowledgement state 1910 and transmits an Acknowledgement message 1911 to the server.

[00205] If there are more blocks to send, the server waits until receiving an Acknowledgement message from the requester. When an Acknowledgement message is received it sends the next block to the requester and again waits for acknowledgement. The requester also repeats the same cycle of states.

[00206] If the server detects a communications failure before sending the last block, it enters a cancellation state 1912 wherein the transaction is cancelled. Similarly, if the requester detects a communications failure before receiving the last block it enters a cancellation state 1913.

[00207] If there are no more blocks to send, the server commits to the transaction and waits for the final Acknowledgement in state 1914. If there is a communications failure

before the server receives the final Acknowledgement message, it still commits to the transaction but includes a report about the event to its credit server in state 1915. This report serves two purposes. It will help legitimize any claims by a user of having been billed for receiving digital works that were not completely received. Also it helps to identify repositories and communications lines that have suspicious patterns of use and interruption. The server then enters its completion state

[00208] On the requester side, when there are no more blocks to receive, the requester commits to the transaction in state 1917. If the requester detects a communications failure at this state, it reports the failure to its credit server in state 1918, but still commits to the transaction. When it has committed, it sends an acknowledgement message to the server. The server then enters its completion state 1919.

[00209] The key property is that both the server and the requester cancel a transaction if it is interrupted before all of the data blocks are delivered, and commits to it if all of the data blocks have been delivered.

[00210] There is a possibility that the server will have sent all of the data blocks (and committed) but the requester will not have received all of them and will cancel the transaction. In this case, both repositories will presumably detect a communications failure and report it to their credit server. This case will probably be rare since it depends on very precise timing of the communications failure. The only consequence will be that the user at the requester repository may want to request a refund from the credit services--and the case for that refund will be documented by reports by both repositories.

[00211] To prevent loss of data, the server should not delete any transferred digital work until receiving the final acknowledgement from the requester. But it also should not use the file. A well known way to deal with this situation is called "two-phase commit" or 2PC.

[00212] Two-phase commit works as follows. The first phase works the same as the method described above. The server sends all of the data to the requester. Both repositories mark the transaction (and appropriate files) as uncommitted. The server sends a ready-to-commit message to the requester. The requester sends back an acknowledgement. The server then commits and sends the requester a commit message. When the requester receives the commit message, it commits the file.

[00213] If there is a communication failure or other crash, the requester must check back with the server to determine the status of the transaction. The server has the last word on

this. The requester may have received all of the data, but if it did not get the final message, it has not committed. The server can go ahead and delete files (except for transaction records) once it commits, since the files are known to have been fully transmitted before starting the 2PC cycle.

[00214] There are variations known in the art which can be used to achieve the same effect. For example, the server could use an additional level of encryption when transmitting a work to a client. Only after the client sends a message acknowledging receipt does it send the key. The client then agrees to pay for the digital work. The point of this variation is that it provides a clear audit trail that the client received the work. For trusted systems, however, this variation adds a level of encryption for no real gain in accountability.

[00215] The transactions for specific usage rights are now discussed.

The Copy Transaction

[00216] A Copy transaction is a request to make one or more independent copies of the work with the same or lesser usage rights. Copy differs from the extraction right discussed later in that it refers to entire digital works or entire folders containing digital works. A copy operation cannot be used to remove a portion of a digital work.

- The requester sends the server a message to initiate the Copy Transaction. This message indicates the work to be copied, the version of the copy right to be used for the transaction, the destination address information (location in a folder) for placing the work, the file data for the work (including its size), and the number of copies requested.

- The repositories perform the common opening transaction steps.

- The server transmits the requested contents and data to the client according to the transmission protocol. If a Next-Set-Of-Rights has been provided in the version of the right, those rights are transmitted as the rights for the work. Otherwise, the rights of the original are transmitted. In any event, the Copy-Count field for the copy of the digital work being sent right is set to the number-of-copies requested.

- The requester records the work contents, data, and usage rights and stores the work. It records the date and time that the copy was made in the properties of the digital work.

- The repositories perform the common closing transaction steps.

The Transfer Transaction

[00217] A Transfer transaction is a request to move copies of the work with the same or lesser usage rights to another repository. In contrast with a copy transaction, this results in removing the work copies from the server.

- The requester sends the server a message to initiate the Transfer Transaction. This message indicates the work to be transferred, the version of the transfer right to be used in the transaction, the destination address information for placing the work, the file data for the work, and the number of copies involved.

- The repositories perform the common opening transaction steps.

- The server transmits the requested contents and data to the requester according to the transmission protocol. If a Next-Set-Of-Rights has been provided, those rights are transmitted as the rights for the work. Otherwise, the rights of the original are transmitted. In either case, the Copy-Count field for the transmitted rights is set to the number-of-copies requested.

- The requester records the work contents, data, and usage rights and stores the work.

- The server decrements its copy count by the number of copies involved in the transaction.

- The repositories perform the common closing transaction steps.

- If the number of copies remaining in the server is now zero, it erases the digital work from its memory.

The Loan Transaction

[00218] A loan transaction is a mechanism for loaning copies of a digital work. The maximum duration of the loan is determined by an internal parameter of the digital work. Works are automatically returned after a predetermined time period.

- The requester sends the server a message to initiate the Transfer Transaction. This message indicates the work to be loaned, the version of the loan right to be used in the transaction, the destination address information for placing the work, the number of copies involved, the file data for the work, and the period of the loan.

- The server checks the validity of the requested loan period, and ends with an error if the period is not valid. Loans for a loaned copy cannot extend beyond the period of the original loan to the server.

- The repositories perform the common opening transaction steps.

- The server transmits the requested contents and data to the requester.

- If a Next-Set-Of-Rights has been provided, those rights are transmitted as the rights for the work. Otherwise, the rights of the original are transmitted, as modified to reflect the loan period.

- The requester records the digital work contents, data, usage rights, and loan period and stores the work.

- The server updates the usage rights information in the digital work to reflect the number of copies loaned out.

- The repositories perform the common closing transaction steps.

- The server updates the usage rights data for the digital work. This may preclude use of the work until it is returned from the loan. The user on the requester platform can now use the transferred copies of the digital work. A user accessing the original repository cannot use the digital work, unless there are copies remaining. What happens next depends on the order of events in time.

[00219] Case 1. If the time of the loan period is not yet exhausted and the requester sends the repository a Return message.

- The return message includes the requester identification, and the transaction ID.

- The server decrements the copies-in-use field by the number of copies that were returned. (If the number of digital works returned is greater than the number actually borrowed, this is treated as an error.) This step may now make the work available at the server for other users.

- The requester deactivates its copies and removes the contents from its memory.

[00220] Case 2. If the time of the loan period is exhausted and the requester has not yet sent a Return message.

- The server decrements the copies-in-use field by the number digital works that were borrowed.

- The requester automatically deactivates its copies of the digital work. It terminates all current uses and erases the digital work copies from memory. One question is why a requester would ever return a work earlier than the period of the loan, since it would be returned automatically anyway. One reason for early return is that there may be a metered fee which determines the cost of the loan. Returning early may reduce that fee.

The Play Transaction

[00221] A play transaction is a request to use the contents of a work. Typically, to “play” a work is to send the digital work through some kind of transducer, such as a speaker

or a display device. The request implies the intention that the contents will not be communicated digitally to any other system. For example, they will not be sent to a printer, recorded on any digital medium, retained after the transaction or sent to another repository.

[00222] This term “play” is natural for examples like playing music, playing a movie, or playing a video game. The general form of play means that a “player” is used to use the digital work. However, the term play covers all media and kinds of recordings. Thus one would “play” a digital work, meaning, to render it for reading, or play a computer program, meaning to execute it. For a digital ticket the player would be a digital ticket agent.

- The requester sends the server a message to initiate the play transaction. This message indicates the work to be played, the version of the play right to be used in the transaction, the identity of the player being used, and the file data for the work.

- The server checks the validity of the player identification and the compatibility of the player identification with the player specification in the right. It ends with an error if these are not satisfactory.

- The repositories perform the common opening transaction steps.

- The server and requester read and write the blocks of data as requested by the player according to the transmission protocol. The requester plays the work contents, using the player.

- When the player is finished, the player and the requester remove the contents from their memory.

- The repositories perform the common closing transaction steps.

The Print Transaction

[00223] A Print transaction is a request to obtain the contents of a work for the purpose of rendering them on a “printer.” We use the term “printer” to include the common case of writing with ink on paper. However, the key aspect of “printing” in our use of the term is that it makes a copy of the digital work in a place outside of the protection of usage rights. As with all rights, this may require particular authorization certificates.

[00224] Once a digital work is printed, the publisher and user are bound by whatever copyright laws are in effect. However, printing moves the contents outside the control of repositories. For example, absent any other enforcement mechanisms, once a digital work is printed on paper, it can be copied on ordinary photocopying machines without intervention by a repository to collect usage fees. If the printer to a digital disk is permitted, then that digital copy is outside of the control of usage rights. Both the creator and the user know this,

although the creator does not necessarily give tacit consent to such copying, which may violate copyright laws.

- The requester sends the server a message to initiate a Print transaction. This message indicates the work to be played, the identity of the printer being used, the file data for the work, and the number of copies in the request.

- The server checks the validity of the printer identification and the compatibility of the printer identification with the printer specification in the right. It ends with an error if these are not satisfactory.

- The repositories perform the common opening transaction steps.
- The server transmits blocks of data according to the transmission protocol.
- The requester prints the work contents, using the printer.
- When the printer is finished, the printer and the requester remove the contents from their memory.

- The repositories perform the common closing transaction steps.

The Backup Transaction

[00225] A Backup transaction is a request to make a backup copy of a digital work, as a protection against media failure. In the context of repositories, secure backup copies differ from other copies in three ways: (1) they are made under the control of a Backup transaction rather than a Copy transaction, (2) they do not count as regular copies, and (3) they are not usable as regular copies. Generally, backup copies are encrypted.

[00226] Although backup copies may be transferred or copied, depending on their assigned rights, the only way to make them useful for playing, printing or embedding is to restore them.

[00227] The output of a Backup operation is both an encrypted data file that contains the contents and description of a work, and a restoration file with an encryption key for restoring the encrypted contents. In many cases, the encrypted data file would have rights for “printing” it to a disk outside of the protection system, relying just on its encryption for security. Such files could be stored anywhere that was physically safe and convenient. The restoration file would be held in the repository. This file is necessary for the restoration of a backup copy. It may have rights for transfer between repositories.

- The requester sends the server a message to initiate a backup transaction. This message indicates the work to be backed up, the version of the backup right to be used in the

transaction, the destination address information for placing the backup copy, the file data for the work.

- The repositories perform the common opening transaction steps.
- The server transmits the requested contents and data to the requester. If a Next-Set-Of-Rights has been provided, those rights are transmitted as the rights for the work. Otherwise, a set of default rights for backup files of the original are transmitted by the server.
- The requester records the work contents, data, and usage rights. It then creates a one-time key and encrypts the contents file. It saves the key information in a restoration file.
- The repositories perform the common closing transaction steps.

[00228] In some cases, it is convenient to be able to archive the large, encrypted contents file to secure offline storage, such as a magneto-optical storage system or magnetic tape. This creation of a non-repository archive file is as secure as the encryption process. Such non-repository archive storage is considered a form of “printing” and is controlled by a print right with a specified “archive-printer.” An archive-printer device is programmed to save the encrypted contents file (but not the description file) offline in such a way that it can be retrieved.

The Restore Transaction

[00229] A Restore transaction is a request to convert an encrypted backup copy of a digital work into a usable copy. A restore operation is intended to be used to compensate for catastrophic media failure. Like all usage rights, restoration rights can include fees and access tests including authorization checks.

- The requester sends the server a message to initiate a Restore transaction. This message indicates the work to be restored, the version of the restore right for the transaction, the destination address information for placing the work, and the file data for the work.
- The server verifies that the contents file is available (i.e. a digital work corresponding to the request has been backed-up.) If it is not, it ends the transaction with an error.
- The repositories perform the common opening transaction steps.
- The server retrieves the key from the restoration file. It decrypts the work contents, data, and usage rights.
- The server transmits the requested contents and data to the requester according to the transmission protocol. If a Next-Set-Of-Rights has been provided, those rights are

transmitted as the rights for the work. Otherwise, a set of default rights for backup files of the original are transmitted by the server.

- The requester stores the digital work.
- The repositories perform the common closing transaction steps.

The Delete Transaction

[00230] A Delete transaction deletes a digital work or a number of copies of a digital work from a repository. Practically all digital works would have delete rights.

- The requester sends the server a message to initiate a delete transaction. This message indicates the work to be deleted, the version of the delete right for the transaction.
- The repositories perform the common opening transaction steps.
- The server deletes the file, erasing it from the file system.
- The repositories perform the common closing transaction steps.

The Directory Transaction

[00231] A Directory transaction is a request for information about folders, digital works, and their parts. This amounts to roughly the same idea as protection codes in a conventional file system like TENEX, except that it is generalized to the full power of the access specifications of the usage rights language.

[00232] The Directory transaction has the important role of passing along descriptions of the rights and fees associated with a digital work. When a user wants to exercise a right, the user interface of his repository implicitly makes a directory request to determine the versions of the right that are available. Typically these are presented to the user--such as with different choices of billing for exercising a right. Thus, many directory transactions are invisible to the user and are exercised as part of the normal process of exercising all rights.

- The requester sends the server a message to initiate a Directory transaction. This message indicates the file or folder that is the root of the directory request and the version of the directory right used for the transaction.

- The server verifies that the information is accessible to the requester.

In particular, it does not return the names of any files that have a HIDE-NAME status in their directory specifications, and it does not return the parts of any folders or files that have HIDE-PARTS in their specification. If the information is not accessible, the server ends the transaction with an error.

- The repositories perform the common opening transaction steps.

- The server sends the requested data to the requester according to the transmission protocol.
- The requester records the data.
- The repositories perform the common closing transaction steps.

The Folder Transaction

[00233] A Folder transaction is a request to create or rename a folder, or to move a work between folders. Together with Directory rights, Folder rights control the degree to which organization of a repository can be accessed or modified from another repository.

- The requester sends the server a message to initiate a Folder transaction. This message indicates the folder that is the root of the folder request, the version of the folder right for the transaction, an operation, and data. The operation can be one of create, rename, and move file. The data are the specifications required for the operation, such as a specification of a folder or digital work and a name.

- The repositories perform the common opening transaction steps.
- The server performs the requested operation--creating a folder, renaming a folder, or moving a work between folders.
- The repositories perform the common closing transaction steps.

The Extract Transaction

[00234] A extract transaction is a request to copy a part of a digital work and to create a new work containing it. The extraction operation differs from copying in that it can be used to separate a part of a digital work from d-blocks or shells that place additional restrictions or fees on it. The extraction operation differs from the edit operation in that it does not change the contents of a work, only its embedding in d-blocks. Extraction creates a new digital work.

- The requester sends the server a message to initiate an Extract transaction. This message indicates the part of the work to be extracted, the version of the extract right to be used in the transaction, the destination address information for placing the part as a new work, the file data for the work, and the number of copies involved.

- The repositories perform the common opening transaction steps.
- The server transmits the requested contents and data to the requester according to the transmission protocol. If a Next-Set-Of-Rights has been provided, those rights are transmitted as the rights for the new work. Otherwise, the rights of the original are transmitted. The Copy-Count field for this right is set to the number-of-copies requested.

- The requester records the contents, data, and usage rights and stores the work. It records the date and time that new work was made in the properties of the work.
- The repositories perform the common closing transaction steps.

The Embed Transaction

[00235] An embed transaction is a request to make a digital work become a part of another digital work or to add a shell d-block to enable the adding of fees by a distributor of the work.

- The requester sends the server a message to initiate an Embed transaction. This message indicates the work to be embedded, the version of the embed right to be used in the transaction, the destination address information for placing the part as a work, the file data for the work, and the number of copies involved.

- The server checks the control specifications for all of the rights in the part and the destination. If they are incompatible, the server ends the transaction with an error.

- The repositories perform the common opening transaction steps.

- The server transmits the requested contents and data to the requester according to the transmission protocol. If a Next-Set-Of-Rights has been provided, those rights are transmitted as the rights for the new work. Otherwise, the rights of the original are transmitted. The Copy-Count field for this right is set to the number-of-copies requested.

- The requester records the contents, data, and usage rights and embeds the work in the destination file.

- The repositories perform the common closing transaction steps.

The Edit Transaction

[00236] An Edit transaction is a request to make a new digital work by copying, selecting and modifying portions of an existing digital work. This operation can actually change the contents of a digital work. The kinds of changes that are permitted depend on the process being used. Like the extraction operation, edit operates on portions of a digital work. In contrast with the extract operation, edit does not effect the rights or location of the work. It only changes the contents. The kinds of changes permitted are determined by the type specification of the processor specified in the rights. In the currently preferred embodiment, an edit transaction changes the work itself and does not make a new work. However, it would be a reasonable variation to cause a new copy of the work to be made.

- The requester sends the server a message to initiate an Edit transaction. This message indicates the work to be edited, the version of the edit right to be used in the

transaction, the file data for the work (including its size), the process-ID for the process, and the number of copies involved.

- The server checks the compatibility of the process-ID to be used by the requester against any process-ID specification in the right. If they are incompatible, it ends the transaction with an error.

- The repositories perform the common opening transaction steps.

- The requester uses the process to change the contents of the digital work as desired. (For example, it can select and duplicate parts of it; combine it with other information; or compute functions based on the information. This can amount to editing text, music, or pictures or taking whatever other steps are useful in creating a derivative work.)

- The repositories perform the common closing transaction steps.

[00237] The edit transaction is used to cover a wide range of kinds of works. The category describes a process that takes as its input any portion of a digital work and then modifies the input in some way. For example, for text, a process for editing the text would require edit rights. A process for “summarizing” or counting words in the text would also be considered editing. For a music file, processing could involve changing the pitch or tempo, or adding reverberations, or any other audio effect. For digital video works, anything which alters the image would require edit rights. Examples would be colorizing, scaling, extracting still photos, selecting and combining frames into story boards, sharpening with signal processing, and so on.

[00238] Some creators may want to protect the authenticity of their works by limiting the kinds of processes that can be performed on them. If there are no edit rights, then no processing is allowed at all. A processor identifier can be included to specify what kind of process is allowed. If no process identifier is specified, then arbitrary processors can be used. For an example of a specific process, a photographer may want to allow use of his photograph but may not want it to be colorized. A musician may want to allow extraction of portions of his work but not changing of the tonality.

Authorization Transactions

[00239] There are many ways that authorization transactions can be defined. In the following, our preferred way is to simply define them in terms of other transactions that we already need for repositories. Thus, it is convenient sometimes to speak of “authorization transactions,” but they are actually made up of other transactions that repositories already have.

[00240] A usage right can specify an authorization-ID, which identifies an authorization object (a digital work in a file of a standard format) that the repository must have and which it must process. The authorization is given to the generic authorization (or ticket) server of the repository which begins to interpret the authorization.

[00241] As described earlier, the authorization contains a server identifier, which may just be the generic authorization server or it may be another server. When a remote authorization server is required, it must contain a digital address. It may also contain a digital certificate.

[00242] If a remote authorization server is required, then the authorization process first performs the following steps:

- The generic authorization server attempts to set up the communications channel. (If the channel cannot be set up, then authorization fails with an error.)
- When the channel is set up, it performs a registration process with the remote repository. (If registration fails, then the authorization fails with an error.)
- When registration is complete, the generic authorization server invokes a “Play” transaction with the remote repository, supplying the authorization document as the digital work to be played, and the remote authorization server (a program) as the “player.” (If the player cannot be found or has some other error, then the authorization fails with an error.)
- The authorization server then “plays” the authorization. This involves decrypting it using either the public key of the master repository that issued the certificate or the session key from the repository that transmitted it. The authorization server then performs various tests. These tests vary according to the authorization server. They include such steps as checking issue and validity dates of the authorization and checking any hot-lists of known invalid authorizations. The authorization server may require carrying out any other transactions on the repository as well, such as checking directories, getting some person to supply a password, or playing some other digital work. It may also invoke some special process for checking information about locations or recent events. The “script” for such steps is contained within the authorization server.
- If all of the required steps are completed satisfactorily, the authorization server completes the transaction normally, signaling that authorization is granted.

The Install Transaction

[00243] An Install transaction is a request to install a digital work as runnable software on a repository. In a typical case, the requester repository is a rendering repository and the

software would be a new kind or new version of a player. Also in a typical case, the software would be copied to file system of the requester repository before it is installed.

- The requester sends the server an Install message. This message indicates the work to be installed, the version of the Install right being invoked, and the file data for the work (including its size).

- The repositories perform the common opening transaction steps.

- The requester extracts a copy of the digital certificate for the software. If the certificate cannot be found or the master repository for the certificate is not known to the requester, the transaction ends with an error.

- The requester decrypts the digital certificate using the public key of the master repository, recording the identity of the supplier and creator, a key for decrypting the software, the compatibility information, and a tamper-checking code. (This step certifies the software.)

- The requester decrypts the software using the key from the certificate and computes a check code on it using a 1-way hash function. If the check-code does not match the tamper-checking code from the certificate, the installation transaction ends with an error. (This step assures that the contents of the software, including the various scripts, have not been tampered with.)

- The requester retrieves the instructions in the compatibility-checking script and follows them. If the software is not compatible with the repository, the installation transaction ends with an error. (This step checks platform compatibility.)

- The requester retrieves the instructions in the installation script and follows them. If there is an error in this process (such as insufficient resources), then the transaction ends with an error. Note that the installation process puts the runnable software in a place in the repository where it is no longer accessible as a work for exercising any usage rights other than the execution of the software as part of repository operations in carrying out other transactions.

- The repositories perform the common closing transaction steps.

The Uninstall Transaction

[00244] An Uninstall transaction is a request to remove software from a repository. Since uncontrolled or incorrect removal of software from a repository could compromise its behavioral integrity, this step is controlled.

- The requester sends the server an Uninstall message. This message indicates the work to be uninstalled, the version of the Uninstall right being invoked, and the file data for the work (including its size).
- The repositories perform the common opening transaction steps.
- The requester extracts a copy of the digital certificate for the software. If the certificate cannot be found or the master repository for the certificate is not known to the requester, the transaction ends with an error.
- The requester checks whether the software is installed. If the software is not installed, the transaction ends with an error.
- The requester decrypts the digital certificate using the public key of the master repository, recording the identity of the supplier and creator, a key for decrypting the software, the compatibility information, and a tamper-checking code. (This step authenticates the certification of the software, including the script for uninstalling it.)
- The requester decrypts the software using the key from the certificate and computes a check code on it using a 1-way hash function. If the check-code does not match the tamper-checking code from the certificate, the installation transaction ends with an error. (This step assures that the contents of the software, including the various scripts, have not been tampered with.)
- The requester retrieves the instructions in the uninstallation script and follows them. If there is an error in this process (such as insufficient resources), then the transaction ends with an error.
- The repositories perform the common closing transaction steps.

DISTRIBUTION AND USE SCENARIOS

[00245] To appreciate the robustness and flexibility of the present invention, various distribution and use scenarios for digital works are illustrated below. These scenarios are meant to be exemplary rather than exhaustive.

Consumers as Unpaid Distributors

[00246] In this scenario, a creator distributes copies of his works to various consumers. Each consumer is a potential distributor of the work. If the consumer copies the digital work (usually for a third party), a fee is collected and automatically paid to the creator.

[00247] This scenario is a new twist for digital works. It depends on the idea that “manufacturing” is just copying and is essentially free. It also assumes that the consumers as distributors do not require a fee for their time and effort in distributing the work.

[00248] This scenario is performed as follows:

[00249] A creator creates a digital work. He grants a Copy right with fees paid back to himself. If he does not grant an Embed right, then consumers cannot use the mechanism to act as distributors to cause fees to be paid to themselves on future copies. Of course, they could negotiate side deals or trades to transfer money on their own, outside of the system.

Paid Distributors

[00250] In another scenario, every time a copy of a digital work is sold a fee is paid to the creator and also to the immediate distributor.

[00251] This scenario does not give special status to any particular distributor. Anyone who sells a document has the right to add a fee to the sale price. The fee for sale could be established by the consumer. It could also be a fixed nominal amount that is contributed to the account of some charity.

[00252] This scenario is performed as follows:

[00253] A creator creates a digital work. He grants a Copy right with fees to be paid back to himself. He grants an Embed right, so that anyone can add shells to have fees paid to themselves.

[00254] A distributor embeds the work in a shell, with fees specified to be paid back to himself. If the distributor is content to receive fees only for copies that he sells himself, he grants an Extract right on the shell.

[00255] When a consumer buys a copy from the distributor, fees are paid both to the distributor and to the creator. If he chooses, the consumer can extract the work from the distributor's shell. He cannot extract it from the creator's shell. He can add his own shell with fees to be paid to himself.

Licensed Distribution

[00256] In this scenario, a creator wants to protect the reputation and value of his work by making certain requirements on its distributors. He issues licenses to distributors that satisfy the requirements, and in turn, promises to reward their efforts by assuring that the work will not be distributed over competing channels. The distributors incur expenses for selecting the digital work, explaining it to buyers, promoting its sale, and possibly for the license itself. The distributor obtains the right to enclose the digital work in a shell, whose

function is to permit the attachment of usage fees to be paid to the distributor in addition to the fees to be paid to the creator.

[00257] This differs from the previous scenario in that it precludes the typical copy owner from functioning as a distributor, since the consumer lacks a license to copy the document. Thus, a consumer cannot make copies, even for free. All copies must come initially from authorized distributors. This version makes it possible to hold distributors accountable in some way for the sales and support of the work, by controlling the distribution of certificates that enable distributors to legitimately charge fees and copy owners to make copies. Since licenses are themselves digital works, the same mechanisms give the creators control over distributors by charging for licenses and putting time limits on their validity.

[00258] This scenario is performed as follows:

[00259] A creator purchases a digital distribution license that he will hand out to his distributors. He puts access requirements (such as a personal license) on the Copy and Transfer rights on the distribution license so that only he can copy or transfer it.

[00260] The creator also creates a digital work. He grants an Embed right and a Copy right, both of which require the distribution license to be exercised. He grants a Play right so that the work can be played by anyone. He may optionally add a Transfer or Loan right, so that end consumers can do some non-commercial exchange of the work among friends.

[00261] A distributor obtains the distribution license and a number of copies of the work. He makes copies for his customers, using his distribution license.

[00262] A customer buys and uses the work. He cannot make new copies because he lacks a distribution license.

Super Distributors

[00263] This is a variation on the previous scenarios. A distributor can sell to anyone and anyone can sell additional copies, resulting in fees being paid back to the creator. However, only licensed distributors can add fees to be paid to themselves.

[00264] This scenario gives distributors the right to add fees to cover their own advertising and promotional costs, without making them be the sole suppliers. Their customers can also make copies, thus broadening the channel without diminishing their revenues. This is because distributors collect fees from copies of any copies that they originally sold. Only distributors can add fees.

[00265] This scenario is performed similarly to the previous ones. There are two key differences. (1) The creator only grants Embed rights for people who have a Distribution license. This is done by putting a requirement for a distributor's license on the Embed right. Consequently, non-distributors cannot add their own fees. (2) The Distributor does not grant Extract rights, so that consumers cannot avoid paying fees to the Distributor if they make subsequent copies. Consequently, all subsequent copies result in fees paid to the Distributor and the Creator.

1-Level Distribution Fees

[00266] In this scenario, a distributor gets a fee for any copy he sells directly. However, if one of his customers sells further copies, he gets no further fee for those copies.

[00267] This scenario pays a distributor only for use of copies that he actually sold.

[00268] This scenario is performed similarly to the previous ones. The key feature is that the distributor creates a shell which specifies fees to be paid to him. He puts Extract rights on the shell. When a consumer buys the work, he can extract away the distributor's shell. Copies made after that will not require fees to be paid to the distributor.

Distribution Trees

[00269] In another scenario, distributors sell to other distributors and fees are collected at each level. Every copy sold by any distributor--even several d-blocks down in the chain--results in a fee being paid back to all of the previous distributors.

[00270] This scenario is like a chain letter or value chain. Every contributor or distributor along the way obtains fees, and is thereby encouraged to promote the sale of copies of the digital work.

[00271] This scenario is performed similarly to the previous ones. The key feature is that the distributor creates a shell which specifies fees to be paid to him. He does not grant Extract rights on the shell. Consequently, all future copies that are made will result in fees paid to him.

Weighted Distribution Trees

[00272] In this scenario, distributors make money according to a distribution tree. The fee that they make depends on various parameters, such as time since their sale or the number of subsequent distributors.

[00273] This is a generalized version of the Distribution Tree scenario, in that it tries to vary the fee to account for the significance of the role of the distributor.

[00274] This scenario is similar to the previous one. The difference is that the fee specification on the distributor's shell has provisions for changes in prices. For example, there could be a fee schedule so that copies made after the passage of time will require lower fees to be paid to the distributor. Alternatively, the distributor could employ a "best-price" billing option, using any algorithm he chooses to determine the fee up to the maximum specified in the shell.

Fees for Reuse

[00275] In this scenario, a first creator creates a work. It is distributed by a first distributor and purchased by a second creator. The second creator extracts a portion of the work and embeds in it a new work distributed by a second distributor. A consumer buys the new work from the second distributor. The first creator receives fees from every transaction; the first distributor receives fees only for his sale; the second creator and second distributor receive fees for the final sale.

[00276] This scenario shows how that flexible automatic arrangements can be set up to create automatic charging systems that mirror current practice. This scenario is analogous to when an author pays a fee to reuse a figure in some paper. In the most common case, a fee is paid to the creator or publisher, but not to the bookstore that sold the book.

[00277] The mechanisms for derived works are the same as those for distribution.

Limited Reuse

[00278] In this scenario, several first creators create works. A second creator makes a selection of these, publishing a collection made up of the parts together with some new interstitial material. (For example, the digital work could be a selection of music or a selection of readings.) The second creator wants to continue to allow some of the selected works to be extractable, but not the interstitial material.

[00279] This scenario deals with fine grained control of the rights and fees for reuse.

[00280] This scenario is performed as follows:

[00281] The first creators create their original works. If they grant extraction and embedding rights, then the second creator can include them in a larger collected work. The second creator creates the interstitial material. He does grant an Extract right on the

interstitial material. He grants Extract rights on a subset of the reused material. A consumer of the collection can only extract portions that have that right. Fees are automatically collected for all parts of the collection.

Commercial Libraries

[00282] Commercial libraries buy works with the right to loan. They limit the loan period and charge their own fees for use. This scenario deals with fees for loaning rather than fees for making copies. The fees are collected by the same automatic mechanisms.

[00283] The mechanisms are the same as previous scenarios except that the fees are associated with the Loan usage right rather than the Copy usage right.

Demo Versions

[00284] A creator believes that if people try his work that they will want to buy it or use it. Consumers of his work can copy the work for free, and play (or execute) a limited version of the work for free, and can play or use the full featured version for a fee. This scenario deals with fees for loaning rather than fees for making copies. The fees are collected by the same automatic mechanisms.

[00285] This scenario is performed as follows:

[00286] The creator creates a digital work and grants various rights and fees. The creator grants Copy and Embed rights without a fee, in order to ensure widespread distribution of the work. Another of the rights is a limited play right with little or no fee attached. For example, this right may be for playing only a portion of the work. The play right can have various restrictions on its use. It could have a ticket that limits the number of times it is used. It could have internal restrictions that limit its functionality. It could have time restrictions that invalidate the right after a period of time or a period of use. Different fees could be associated with other versions of the Play right.

Upgrading a Digital Work with a Vendor

[00287] A consumer buys a digital work together with an agreement that he can upgrade to a new version at a later date for a modest fee, much less than the usual purchase price. When the new version becomes available, he goes to a qualified vendor to make the transaction.

[00288] This scenario deals with a common situation in computer software. It shows how a purchase may include future “rights.” Two important features of the scenario are that

the transaction must take place at a qualified vendor, and that the transaction can be done only once per copy of the digital work purchased.

[00289] This scenario is performed as follows:

[00290] The creator creates a digital work, an upgrade ticket, and a distribution license. The upgrade ticket uses the a generic ticket agent that comes with repositories. As usual, the distribution license does not have Copy or Transfer rights. He distributes a bundled copies of the work and the ticket to his distributors as well as distribution licenses.

[00291] The distributor sells the old bundled work and ticket to customers.

[00292] The customer extracts the work and the ticket. He uses the work according to the agreements until the new version becomes available.

[00293] When the new work is ready, the creator gives it to distributors. The new work has a free right to copy from a distributor if a ticket is available.

[00294] The consumer goes to distributors and arranges to copy the work. The transaction offers the ticket. The distributor's repository punches the ticket and copies the new version to the consumer's repository.

[00295] The consumer can now use the new version of the work.

Distributed Upgrading of Digital Works

[00296] A consumer buys a digital work together with an agreement that he can upgrade to a new version at a later date for a modest fee, much less than the usual purchase price. When the new version becomes available, he goes to anyone who has the upgraded version and makes the transaction.

[00297] This scenario is like the previous one in that the transaction can only be done once per copy of the digital work purchased, but the transaction can be accomplished without the need to connect to a licensed vendor.

[00298] This scenario is similar to the previous one except that the Copy right on the new work does not require a distribution license. The consumer can upgrade from any repository having the new version. He cannot upgrade more than once because the ticket cannot work after it has been punched. If desired, the repository can record the upgrade transaction by posting a zero cost bill to alert the creator that the upgrade has taken place.

Limited Printing

[00299] A consumer buys a digital work and wants to make a few ephemeral copies. For example, he may want to print out a paper copy of part of a digital newspaper, or he may want to make a (first generation) analog cassette tape for playing in his car. He buys the digital work together with a ticket required for printing rights.

[00300] This scenario is like the common practice of people making cassette tapes to play in their car. If a publisher permits the making of cassette tapes, there is nothing to prevent a consumer from further copying the tapes. However, since the tapes are “analog copies,” there is a noticeable quality loss with subsequent generations. The new contribution of the present invention is the use of tickets in the access controls for the making of the analog copies.

[00301] This scenario is performed as follows:

[00302] The creator sells a work together with limited printing rights. The printing rights specify the kind of printer (e.g., a kind of cassette recorder or a kind of desktop paper printer) and also the kind of ticket required. The creator either bundles a limited number of tickets or sells them separately. If the tickets use the generic ticket agent, the consumer with the tickets can exercise the right at his convenience.

Demand Publishing

[00303] Professors in a business school want to put together course books of readings selected from scenario studies from various sources. The bookstore wants to be able to print the books from digital masters, without negotiating for and waiting for approval of printing of each of the scenarios. The copyright holders of the scenarios want to be sure that they are paid for every copy of their work that is printed.

[00304] On many college campuses, the hassle of obtaining copy clearances in a timely way has greatly reduced the viability of preparing course books. Print shops have become much more cautious about copying works in the absence of documented permission.

[00305] Demand Publishing is performed as follows: the creator sells a work together with printing rights for a fee. There can be rights to copy (distribute) the work between bookstore repositories, with or without fee. The printing rights specify the kind of printer. Whenever a bookstore prints one of the works (either standalone or embedded in a collection), the fee is credited to the creator automatically. To discourage unauthorized copying of the print outs, it would be possible for the printer to print tracer messages discretely on the pages identifying the printing transaction, the copy number, and any other

identifying information. The tracer information could be secretly embedded in the text itself (encoded in the grey scale) or hidden in some other way.

Metered Use and Multiple Price Packages

[00306] A consumer does not know what music to purchase until he decides whether he likes it. He would like to be able to take it home and listen to it, and then decide whether to purchase. Furthermore, he would like the flexibility of paying less if he listens to it very infrequently.

[00307] This scenario just uses the capability of the approach to have multiple versions of a right on a digital work. Each version of the right has its own billing scheme. In this scenario, the creator of the work can offer the Copy right without fee, and defer billing to the exercise of the Play right. One version of the play right would allow a limited performance without fee--a right to "demo". Another version of the right could have a metered rate, of say \$0.25 per hour of play. Another version could have a fee of \$15.00 for the first play, but no fee for further playing. When the consumer exercises a play right, he specifies which version of the right is being selected and is billed accordingly.

Fees for Font Usage

[00308] A designer of type fonts invests several months in the design of special fonts. The most common way of obtaining revenue for this work is to sell copies of the fonts to publishers for unlimited use over unlimited periods of time. A font designer would like to charge a rate that reflects the amount that the font is used.

[00309] This scenario is performed as follows: the font designer creates a font as a digital work. He creates versions of the Play right that bill either for metered use or "per-use". Each version of the play right would require that the player (a print layout program) be of an approved category. The font designer assigns appropriate fees to exercise the Copy right. When a publisher client wants to use a font, he includes it as input to a layout program, and is billed automatically for its use. In this way, a publisher who makes little use of a font pays less than one who uses it a lot.

Rational Database Usage Charges

[00310] Online information retrieval services typically charge for access in a way that most clients find unpredictable and uncorrelated to value or information use. The fee depends on which databases are open, dial-up connect time, how long the searches require, and which articles are printed out. There are no provisions for extracting articles or photographs, no

method for paying to reuse information in new works, no distinction between having the terminal sit idly versus actively searching for data, no distinction between reading articles on the screen and doing nothing, and higher rates per search when the centralized facility is busy and slow servicing other clients. Articles can not be offloaded to the client's machine for off-site search and printing. To offer such billing or the expanded services, the service company would need a secure way to account for and bill for how information is used.

[00311] This scenario is performed as follows:

[00312] The information service bundles its database as files in a repository. The information services company assigns different fees for different rights on the information files. For example, there could be a fee for copying a search database or a source file and a different fee for printing. These fees would be in addition to fees assigned by the original creator for the services. The fees for using information would be different for using them on the information service company's computers or the client's computers. This billing distinction would be controlled by having different versions of the rights, where the version for use on the service company's computer requires a digital certificate held locally. Fees for copying or printing files would be handled in the usual way, by assigning fees to exercising those rights. The distinction between searching and viewing information would be made by having different "players" for the different functions. This distinction would be maintained on the client's computers as well as the service computers. Articles could be extracted for reuse under the control of Extract and Embed rights. Thus, if a client extracts part of an article or photograph, and then sells copies of a new digital work incorporating it, fees could automatically be collected both by the information service and earlier creators and distributors of the digital work. In this way, the information retrieval service could both offer a wider selection of services and billing that more accurately reflects the client's use of the information.

Print Spooling with Rights

[00313] In the simplest scenario, when a user wants to print a digital document he issues a print command to the user interface. If the document has the appropriate rights and the conditions are satisfied, the user agrees to the fee and the document is printed. In other cases, the printer may be on a remote repository and it is convenient to spool the printing to a later time. This leads to several issues. The user requesting the printing wants to be sure that he is not billed for the printing until the document is actually printed. Restated, if he is billed at the time the print job is spooled but the job is canceled before printing is done, he does not

want to pay. Another issue is that when spooling is permitted, there are now two times at which rights, conditions and fees could be checked: the time at which a print job is spooled and the time at which a print is made. As with all usage rights, it is possible to have rights that expire and to have rights whose fee depends on various conditions. What is needed is a means to check rights and conditions at the time that printing is actually done.

[00314] This scenario is performed as follows: A printing repository is a repository with the usual repository characteristics plus the hardware and software to enable printing. Suppose that a user logs into a home repository and wants to spool print jobs for a digital work at a remote printing repository. The user interface for this could treat this as a request to “spool” prints. Underneath this “spooling” request, however, are standard rights and requests. To support such requests, the creator of the work provides a Copy right, which can be used to copy the work to a printing repository. In the default case, this Copy right would have no fees associated for making the copy. However, the Next-Set-Of-Rights for the copy would only include the Print rights, with the usual fees for each variation of printing. This version of the Copy right could be called the “print spooling” version of the Copy right. The user’s “spool request” is implemented as a Copy transaction to put a copy of the work on the printing repository, followed by Print transactions to create the prints of the work. In this way, the user is only billed for printing that is actually done. Furthermore, the rights, conditions and fees for printing the work are determined when the work is about to be printed.

[00315] Thus, a system for enforcing the usage rights of digital works is disclosed. While the embodiments disclosed herein are preferred, it will be appreciated from this teaching that various alternative, modifications, variations or improvements therein may be made by those skilled in the art, which are intended to be encompassed by the following claims.

APPENDIX A
GLOSSARY

AUTHORIZATION REPOSITORY:

[00316] A special type of repository which provides an authorization service. An authorization may be specified by a usage right. The authorization must be obtained before the right may be exercised.

BILLING CLEARINGHOUSE:

[00317] A financial institution or the like whose purpose is to reconcile billing information received from credit servers. The billing clearinghouse may generate bills to users or alternatively, credit and debit accounts involved in the commercial transactions.

BILLING TRANSACTIONS:

[00318] The protocol used by which a repository reports billing information to a credit server.

CLEARINGHOUSE TRANSACTIONS:

[00319] The protocol used between a credit server and a clearinghouse.

COMPOSITE DIGITAL WORK:

[00320] A digital work comprised of distinguishable parts. Each of the distinguishable parts is itself a digital work which has usage rights attached.

CONTENT:

[00321] The digital information (i.e. raw bits) representing a digital work.

COPY OWNER:

[00322] A term which refers to the party who owns a digital work stored in a repository. In the typical case, this party has purchased various rights to the document for printing, viewing, transferring, or other specific uses.

CREATOR:

[00323] A term which refers to a party who produces a digital work.

CREDIT SERVER:

[00324] A device which collects and reports billing information for a repository. In many implementations, this could be built as part of a repository. It requires a means for periodically communicating with a billing clearinghouse.

DESCRIPTION TREE:

[00325] A structure which describes the location of content and the usage rights and usage fees for a digital work. A description tree is comprised of description blocks. Each description block corresponds to a digital work or to an interest (typically a revenue bearing interest) in a digital work.

DIGITAL WORK (WORK):

[00326] Any encapsulated digital information. Such digital information may represent music, a magazine or book, or a multimedia composition. Usage rights and fees are attached to the digital work.

DISTRIBUTOR:

[00327] A term which refers to a party who legitimately obtains a copy of a digital work and offers it for sale.

IDENTIFICATION (DIGITAL) CERTIFICATE:

[00328] A signed digital message that attests to the identity of the possessor. Typically, digital certificates are encrypted in the private key of a well-known master repository.

MASTER REPOSITORY:

[00329] A special type of repository which issues identification certificates and distributes lists of repositories whose integrity have been compromised and which should be denied access to digital works (referred to as repository “hotlists”).

PUBLIC KEY ENCRYPTION:

[00330] An encryption technique used for secure transmission of messages on a communication channel. Key pairs are used for the encryption and decryption of messages. Typically one key is referred to as the public key and the other is the private key. The keys are inverses of each other from the perspective of encryption. Restated, a digital work that is encrypted by one key in the pair can be decrypted only by the other.

REGISTRATION TRANSACTIONS:

[00331] The protocol used between repositories to establish a trusted session.

RENDERING REPOSITORY:

[00332] A special type of repository which is typically coupled to a rendering system. The rendering repository will typically be embodied within the secure boundaries of a rendering system.

RENDERING SYSTEM:

[00333] The combination of a rendering repository and a rendering device. Examples of a rendering systems include printing systems, display systems, general purpose computer systems, video systems or audio systems.

REPOSITORY:

[00334] Conceptually a set of functional specifications defining core functionality in the support of usage rights. A repository is a trusted system in that it maintains physical, communications and behavioral integrity.

REQUESTER MODE:

[00335] A mode of a repository where it is requesting access to a digital work.

REVENUE OWNERS:

[00336] A term which refers to the parties that maintain an interest in collecting fees for document use or who stand to lose revenue if illegitimate copies of the digital work are made.

SERVER MODE:

[00337] A mode of a repository where it is processing an incoming request to access a digital work.

SHELL DESCRIPTION BLOCK:

[00338] A special type of description block designating an interest in a digital work, but which does not add content. This will typically be added by a distributor of a digital work to add their fees.

TRANSACTIONS:

[00339] A term used to refer to the protocols by which repositories communicate.

USAGE FEES:

[00340] A fee charged to a requester for access to a digital work. Usage fees are specified within the usage rights language.

USAGE RIGHTS:

[00341] A language for defining the manner in which a digital work may be used or distributed, as well as any conditions on which use or distribution is premised.

USAGE TRANSACTIONS:

[00342] A set of protocols by which repositories communicate in the exercise of a usage rights. Each usage right has it's own transaction steps.

WHAT IS CLAIMED:

1. A computer-implemented method of distributing digital content to at least one recipient computing device to be rendered by the at least one recipient computing device in accordance with usage rights information, the method comprising:

determining, by at least one sending computing device, if the at least one recipient computing device is trusted to receive the digital content from the at least one sending computing device;

sending the digital content, by the at least one sending computing device, to the at least one recipient computing device only if the at least one recipient computing device has been determined to be trusted to receive the digital content from the at least one sending computing device; and

sending usage rights information indicating how the digital content may be rendered by the at least one recipient computing device, the usage rights information being enforceable by the at least on recipient computing device.

2. The method of claim 1, wherein the usage rights information further includes a condition under which the content can be rendered.

3. The method of claim 1, wherein the determination of trust comprises:

receiving a request from at least one recipient computing device for an authorization object required to render the digital content; and

transmitting the authorization object to the at least one recipient computing device when it is determined that the request should be granted.

4. The method of claim 1, wherein the determination of trust comprises:

receiving a registration message from the at least one recipient device, the registration message including an identification certificate of the recipient computing device and a random registration identifier, the identification certificate being certified by a master device;

validating the authenticity of the at least one recipient device;

exchanging messages including at least one session key with the at least one recipient device, the session key to be used in communications; and

conducting a secure transaction using the session key, wherein the secure transaction includes sending the digital content to the at least one recipient device.

5. The method of claim 10, wherein the validating comprises:
- verifying the identification certificate of the at least one recipient device;
 - generating a message to test the authenticity of the at least one recipient device, the generated message including a nonce;
 - sending the generated message to the at least one recipient device; and
 - verifying if the at least one recipient device correctly processed the generated message.
6. A sending apparatus for distributing digital content to at least one recipient computing device to be rendered by the at least one recipient computing device in accordance with usage rights information, the sending apparatus comprising:
- one or more processors; and
 - one or more memories operatively coupled to at least one of the one or more processors and having instructions stored thereon that, when executed by at least one of the one or more processors, cause at least one of the one or more processors to:
 - determine if the at least one recipient computing device is trusted to receive the digital content from the sending apparatus;
 - send the digital content, by the sending apparatus, to the at least one recipient computing device only if the at least one recipient computing device has been determined to be trusted to receive the digital content from the sending apparatus; and
 - send usage rights information indicating how the digital content may be rendered by the at least one recipient computing device, the usage rights information being enforceable by the at least on recipient computing device.
7. The apparatus of claim 6, wherein the usage rights information further includes a condition under which the content can be rendered.
8. The apparatus of claim 6, wherein the determination of trust comprises:
- receiving a request from at least one recipient computing device for an authorization object required to render the digital content; and
 - transmitting the authorization object to the at least one recipient computing device when it is determined that the request should be granted.

9. The apparatus of claim 6, wherein the determination of trust comprises:

receiving a registration message from the at least one recipient device, the registration message including an identification certificate of the recipient computing device and a random registration identifier, the identification certificate being certified by a master device;

validating the authenticity of the at least one recipient device;

exchanging messages including at least one session key with the at least one recipient device, the session key to be used in communications; and

conducting a secure transaction using the session key, wherein the secure transaction includes sending the digital content to the at least one recipient device.

10. The apparatus of claim 9, wherein the validating comprises:

verifying the identification certificate of the at least one recipient device;

generating a message to test the authenticity of the at least one recipient device, the generated message including a nonce;

sending the generated message to the at least one recipient device; and

verifying if the at least one recipient device correctly processed the generated message.

11. At least one non-transitory computer-readable medium storing computer-readable instructions that, when executed by at least one sending computing device, cause the at least one sending computing device to:

determine if the at least one recipient computing device is trusted to receive the digital content from the at least one sending computing device;

send the digital content, by the at least one sending computing device, to the at least one recipient computing device only if the at least one recipient computing device has been determined to be trusted to receive the digital content from the at least one sending computing device; and

send usage rights information indicating how the digital content may be rendered by the at least one recipient computing device, the usage rights information being enforceable by the at least one recipient computing device.

12. The at least one non-transitory computer-readable medium of claim 11, wherein the usage rights information further includes a condition under which the content can be rendered.

13. The at least one non-transitory computer-readable medium of claim 11, wherein the determination of trust comprises:

- receiving a request from at least one recipient computing device for an authorization object required to render the digital content; and
- transmitting the authorization object to the at least one recipient computing device when it is determined that the request should be granted.

14. The at least one non-transitory computer-readable medium of claim 11, wherein the determination of trust comprises:

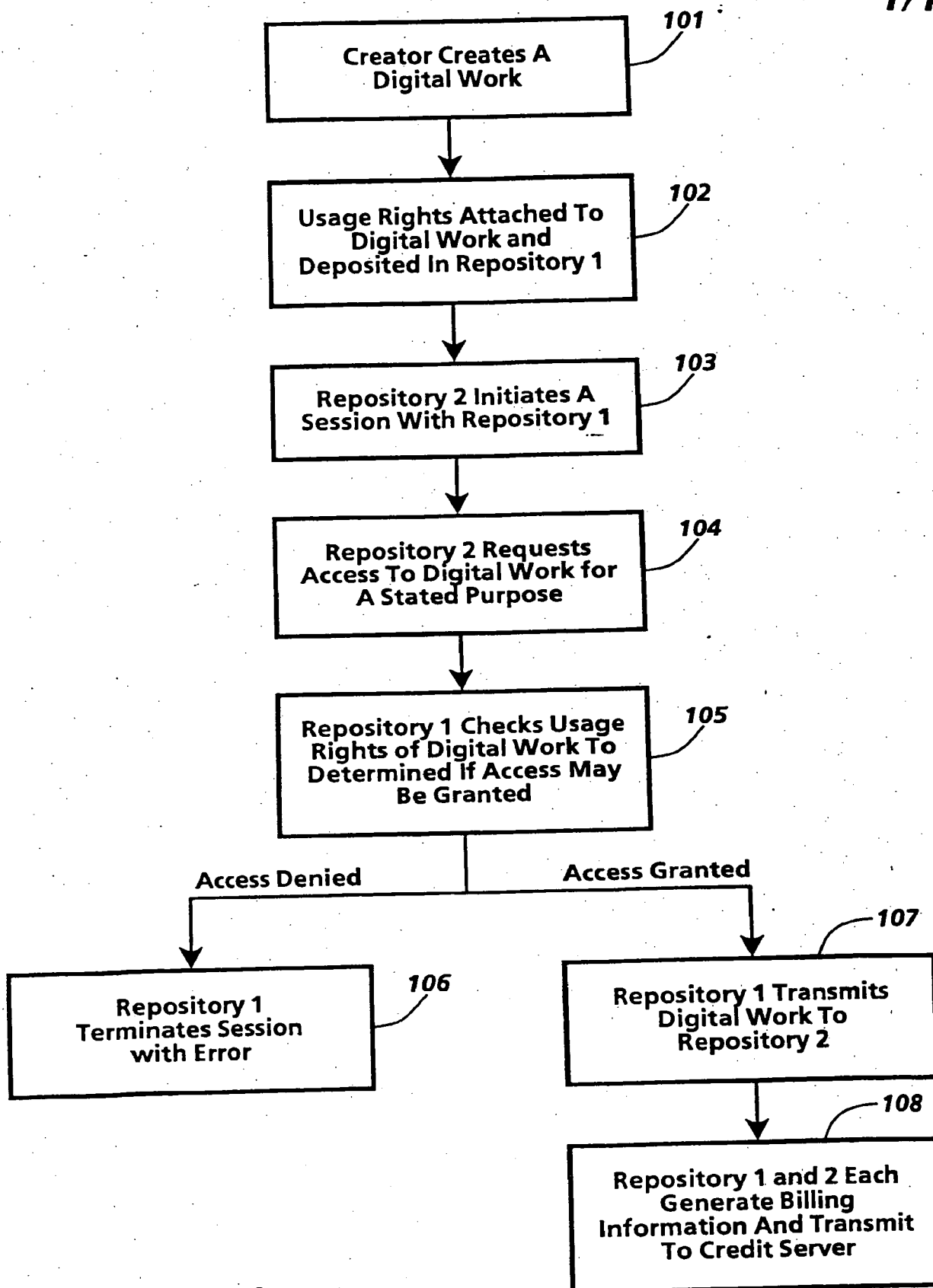
- receiving a registration message from the at least one recipient device, the registration message including an identification certificate of the recipient computing device and a random registration identifier, the identification certificate being certified by a master device;
- validating the authenticity of the at least one recipient device;
- exchanging messages including at least one session key with the at least one recipient device, the session key to be used in communications; and
- conducting a secure transaction using the session key, wherein the secure transaction includes sending the digital content to the at least one recipient device.

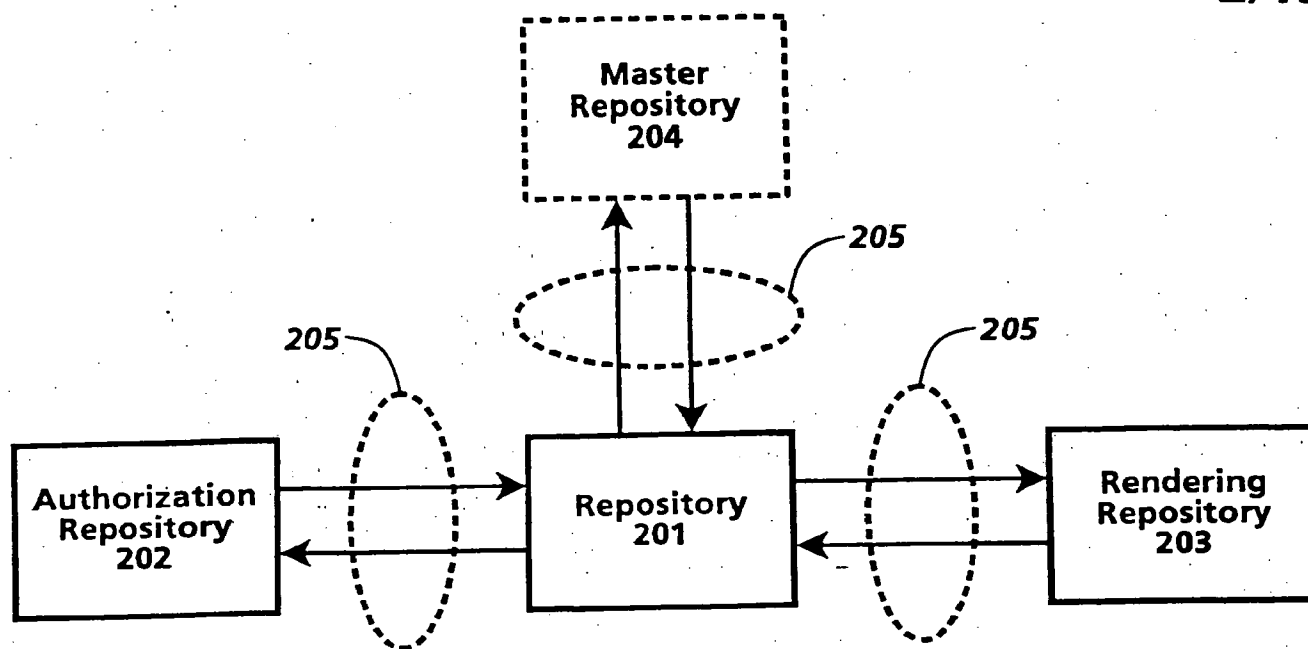
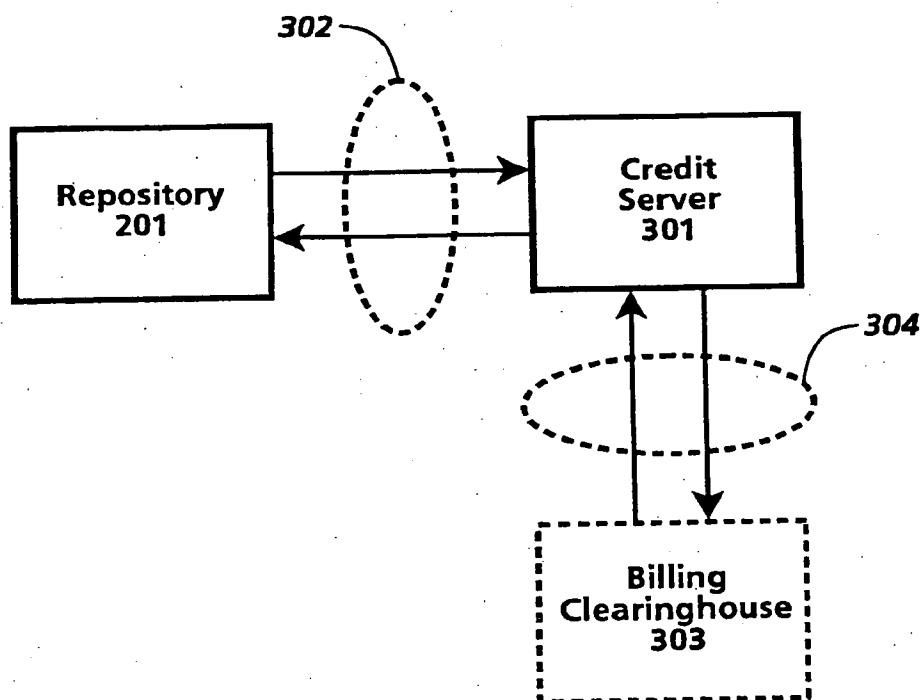
15. The at least one non-transitory computer-readable medium of claim 14, wherein the validating comprises:

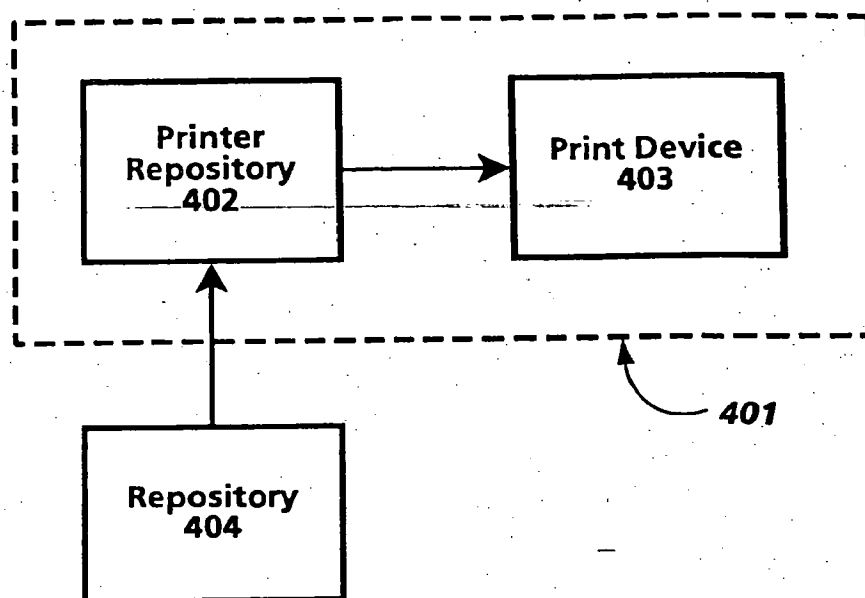
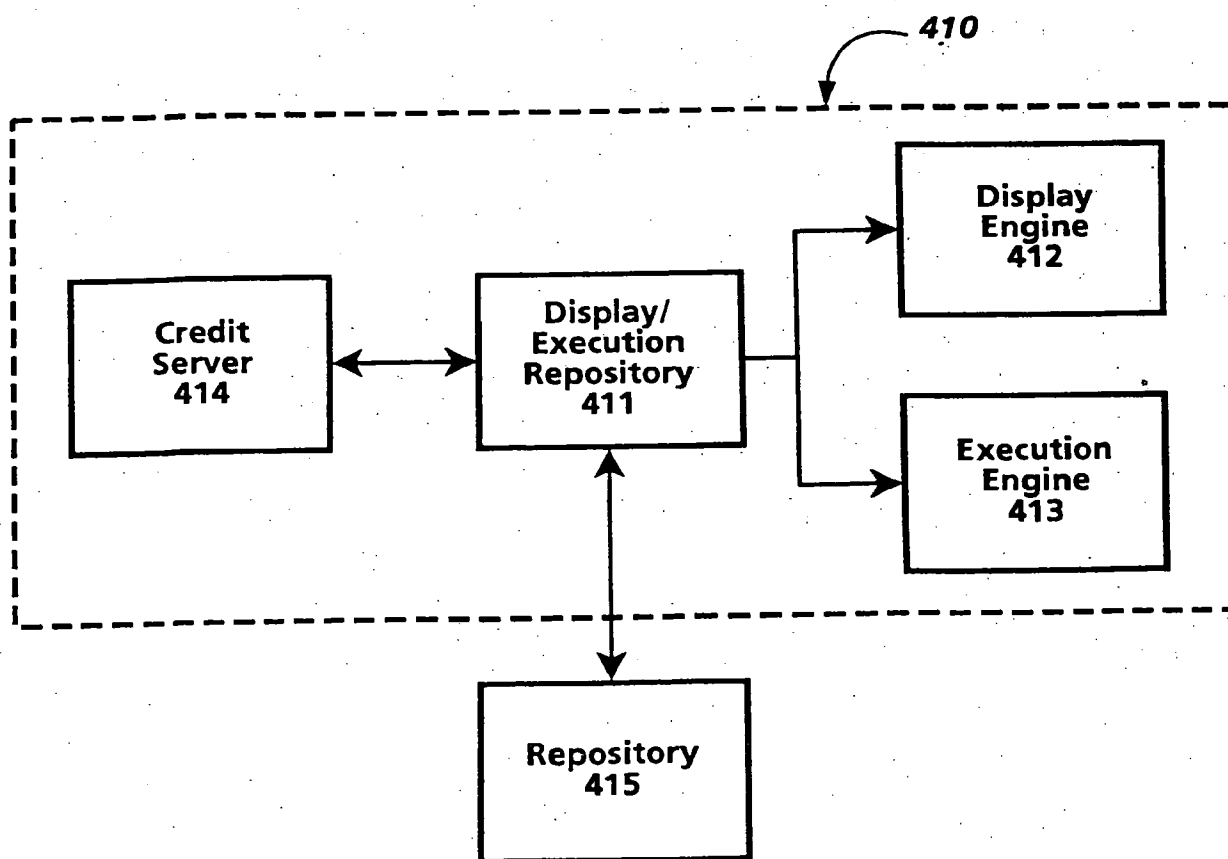
- verifying the identification certificate of the at least one recipient device;
- generating a message to test the authenticity of the at least one recipient device, the generated message including a nonce;
- sending the generated message to the at least one recipient device; and
- verifying if the at least one recipient device correctly processed the generated message.

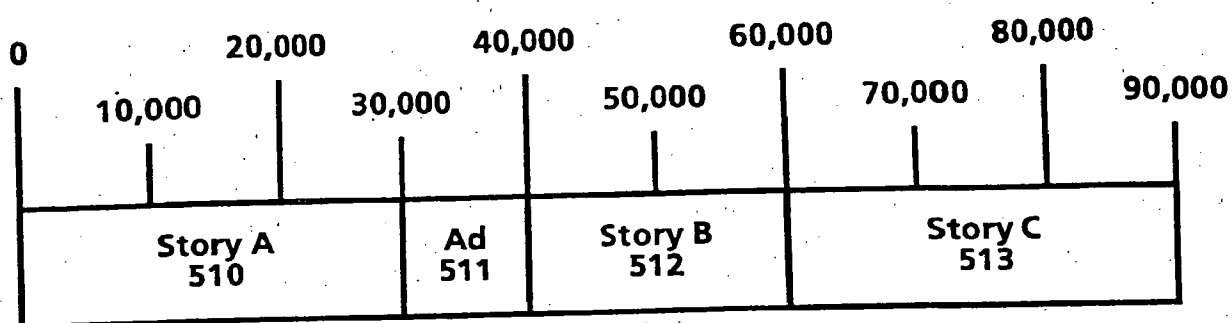
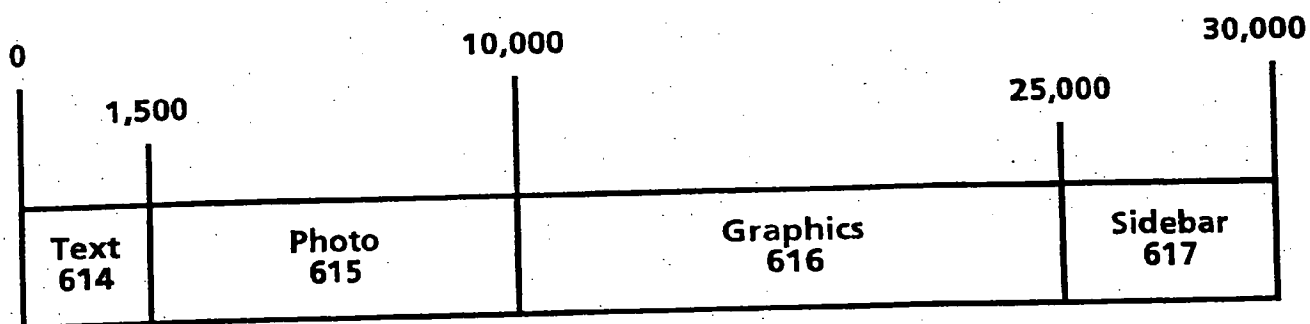
ABSTRACT OF THE DISCLOSURE

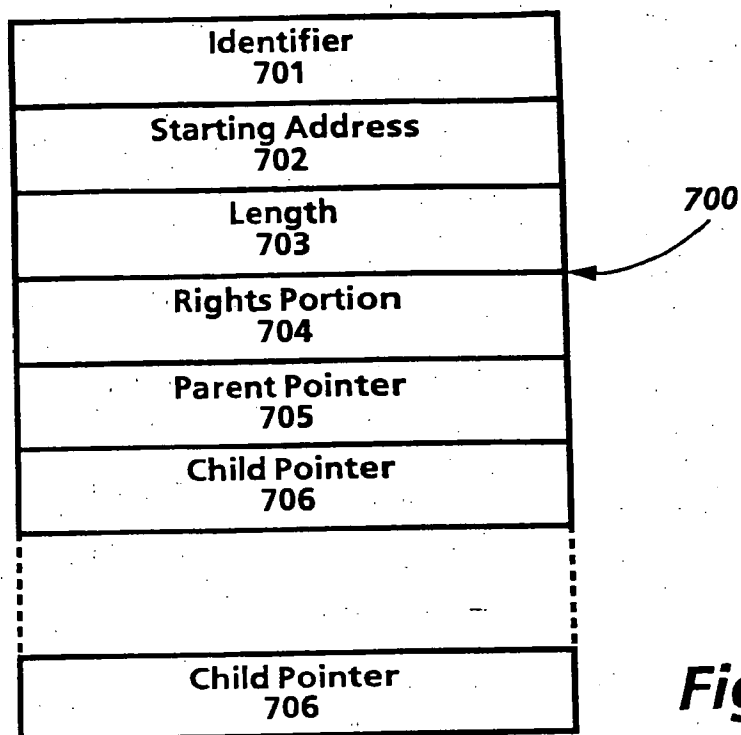
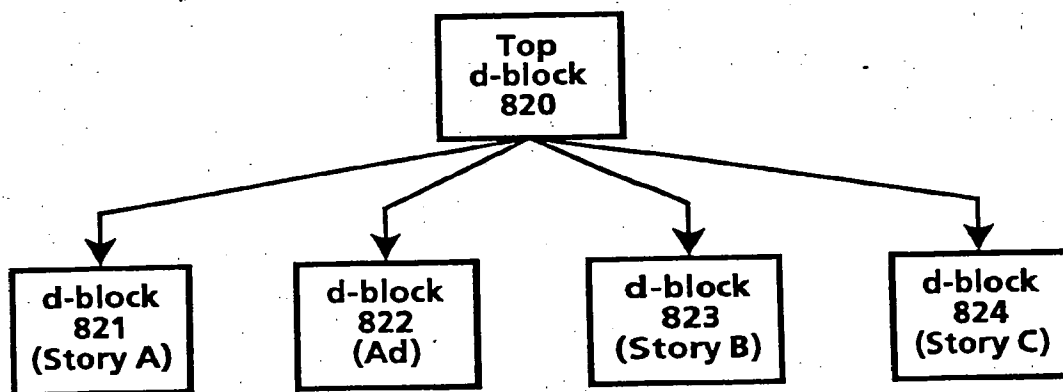
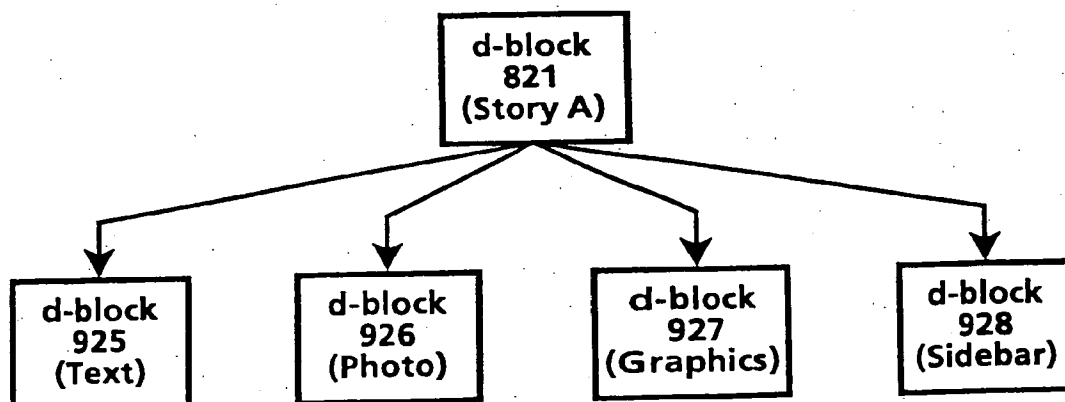
Methods, apparatus, and media for distributing digital content to at least one recipient computing device to be rendered by the at least one recipient computing device in accordance with usage rights information. An exemplary method comprises determining, by at least one sending computing device, if the at least one recipient computing device is trusted to receive the digital content from the at least one sending computing device, sending the digital content, by the at least one sending computing device, to the at least one recipient computing device only if the at least one recipient computing device has been determined to be trusted to receive the digital content from the at least one sending computing device, and sending usage rights information indicating how the digital content may be rendered by the at least one recipient computing device, the usage rights information being enforceable by the at least one recipient computing device.

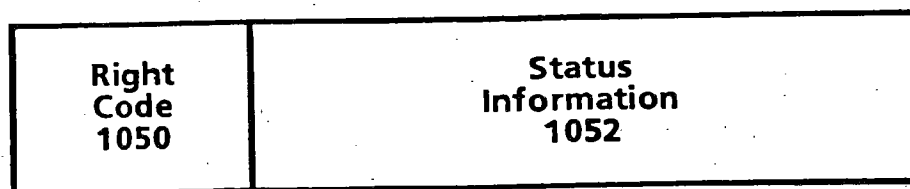
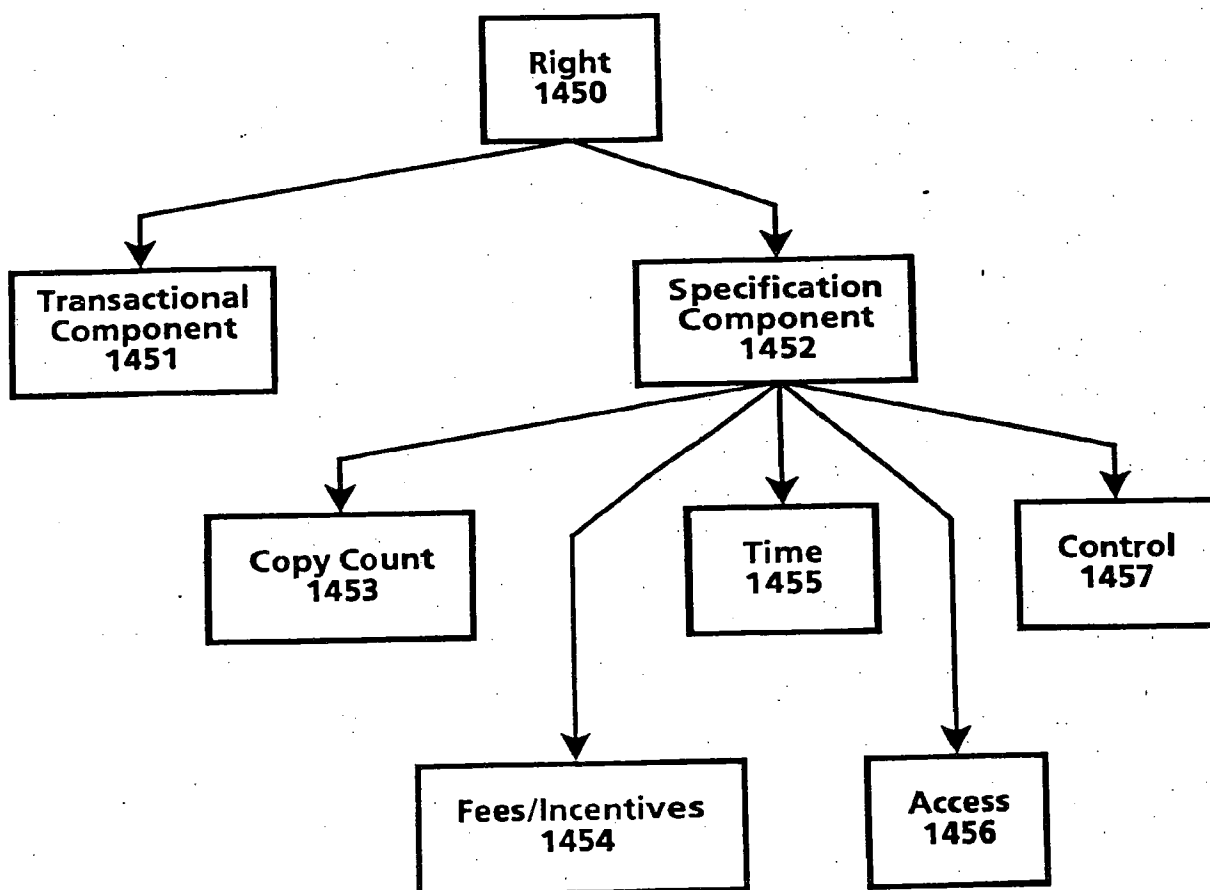
**Fig. 1**

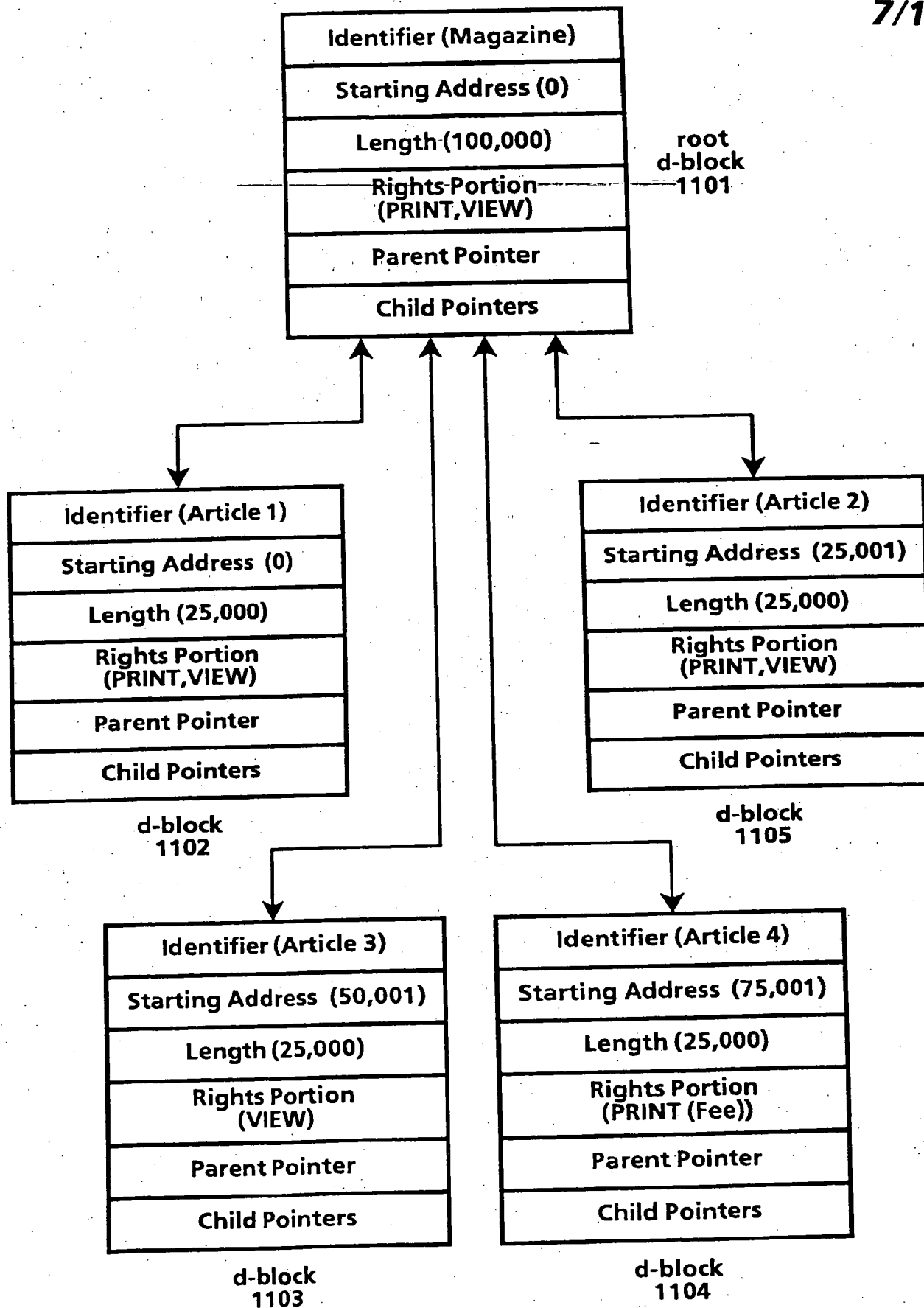
**Fig. 2****Fig. 3**

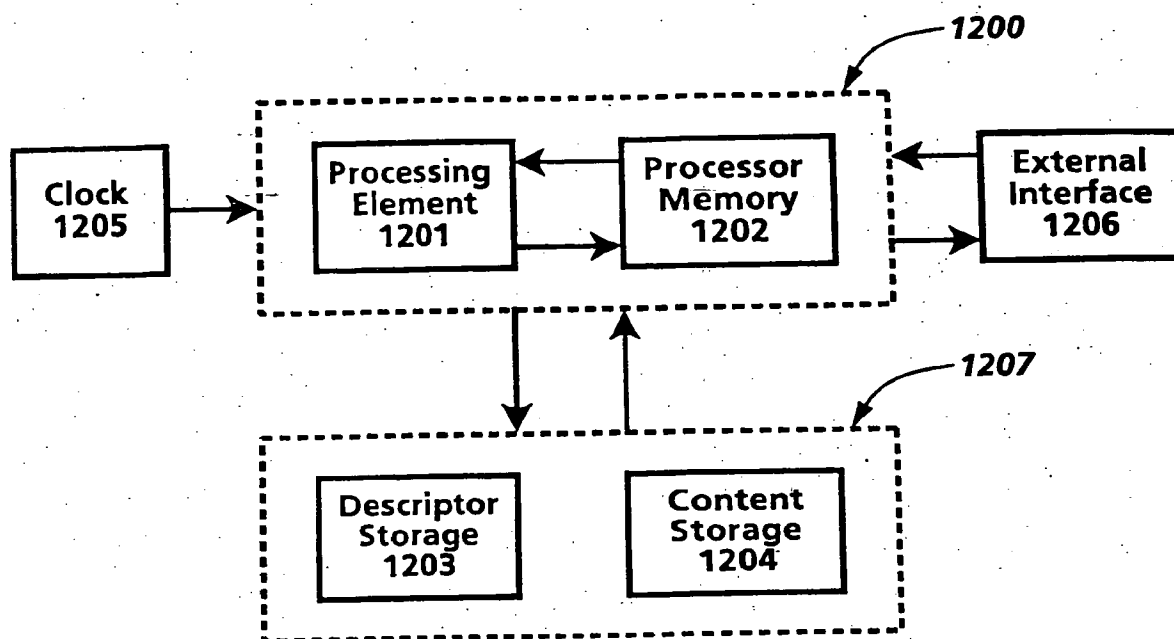
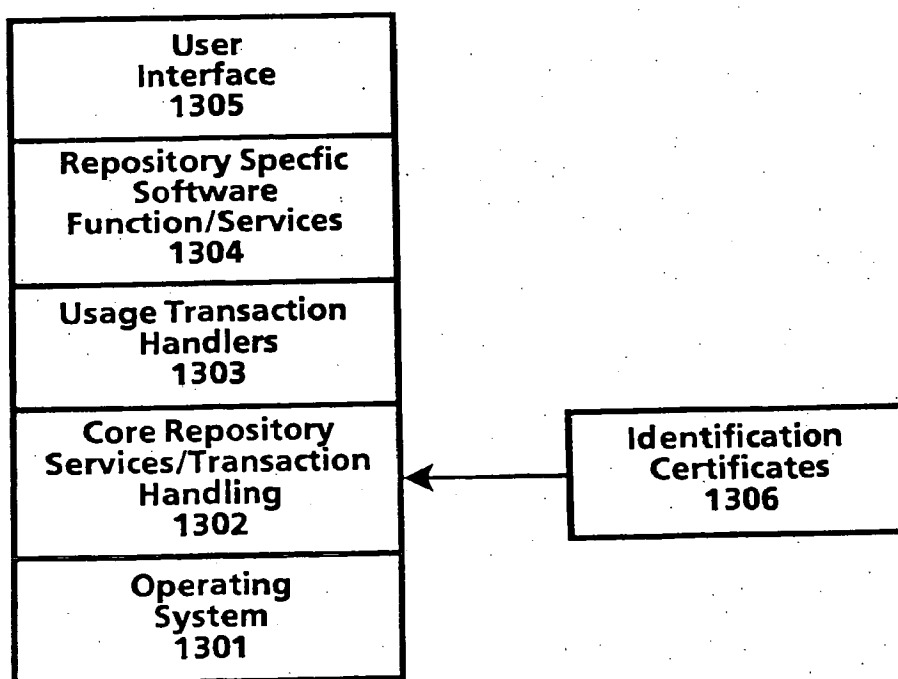
**Fig. 4a****Fig. 4b**

**Fig. 5****Fig. 6**

**Fig. 7****Fig. 8****Fig. 9**

**Fig.10****Fig.14**

**Fig. 11**

**Fig.12****Fig.13**

- 1501 ~ Digital Work Rights := (Rights*)
- 1502 ~ Right := (Right-Code {Copy-Count} {Control-Spec} {Time-Spec}
 {Access-Spec} {Fee-Spec})
- 1503 ~ Right-Code := Render-Code | Transport-Code | File-Management-
 Code | Derivative-Works-Code | Configuration-Code
- 1504 ~ Render-Code := [Play: {Player: Player-ID} | Print: {Printer: Printer-ID}]
- 1505 ~ Transport-Code := [Copy | Transfer | Loan {Remaining-Rights:
 Next-Set-of-Rights}]{(Next-Copy-Rights: Next-Set-of-Rights)}
- 1506 ~ File-Management-Code := Backup {Back-Up-Copy-Rights:
 Next-Set-of-Rights} | Restore | Delete | Folder
 | Directory {Name: Hide-Local | Hide-Remote}
 | Parts: Hide-Local | Hide-Remote}
- 1507 ~ Derivative-Works-Code := [Extract | Embed | Edit {Process:
 Process-ID}] {Next-Copy-Rights:
 Next-Set-of-Rights}
- 1508 ~ Configuration-Code := Install | Uninstall
- 1509 ~ Next-Set-of-Rights := {(Add: Set-Of-Rights)} {(Delete:
 Set-Of-Rights)} {(Replace: Set-Of-Rights)} {(Keep: Set-Of-Rights)}
- 1510 ~ Copy-Count := (Copies: positive-integer | 0 | Unlimited)
- 1511 ~ Control-Spec := (Control: {Restrictable | Unrestrictable}
 {Unchargeable | Chargeable})
- 1512 ~ Time-Spec := ({Fixed-Interval | Sliding-Interval | Meter-Time}
 Until: Expiration-Date)
- 1513 ~ Fixed-Interval := From: Start-Time
- 1514 ~ Sliding-Interval := Interval: Use-Duration
- 1515 ~ Meter-Time := Time-Remaining: Remaining-Use
- 1516 ~ Access-Spec := ({SC: Security-Class} {Authorization: Authorization-ID*}
 {Other-Authorization: Authorization-ID*} {Ticket: Ticket-ID})
- 1517 ~ Fee-Spec := {Scheduled-Discount} Regular-Fee-Spec | Scheduled-Fee-Spec |
 Markup-Spec
- 1518 ~ Scheduled-Discount := Scheduled-Discount: (Scheduled-Discount:
 (Time-Spec Percentage)*)
- 1519 ~ Regular-Fee-Spec := ({Fee: | Incentive: } [Per-Use-Spec | Metered-Rate-
 Spec | Best-Price-Spec | Call-For-Price-Spec]
 {Min: Money-Unit Per: Time-Spec} {Max:
 Money-Unit Per: Time-Spec} To: Account-ID)
- 1520 ~ Per-Use-Spec := Per-Use: Money-unit
- 1521 ~ Metered-Rate-Spec := Metered: Money-Unit Per: Time-Spec
- 1522 ~ Best-Price-Spec := Best-Price: Money-unit Max: Money-unit
- 1523 ~ Call-For-Price-Spec := Call-For-Price
- 1524 ~ Scheduled-Fee-Spec := (Schedule: (Time-Spec Regular-Fee-Spec)*)
- 1525 ~ Markup-Spec := Markup: percentage To: Account-ID

Fig. 15

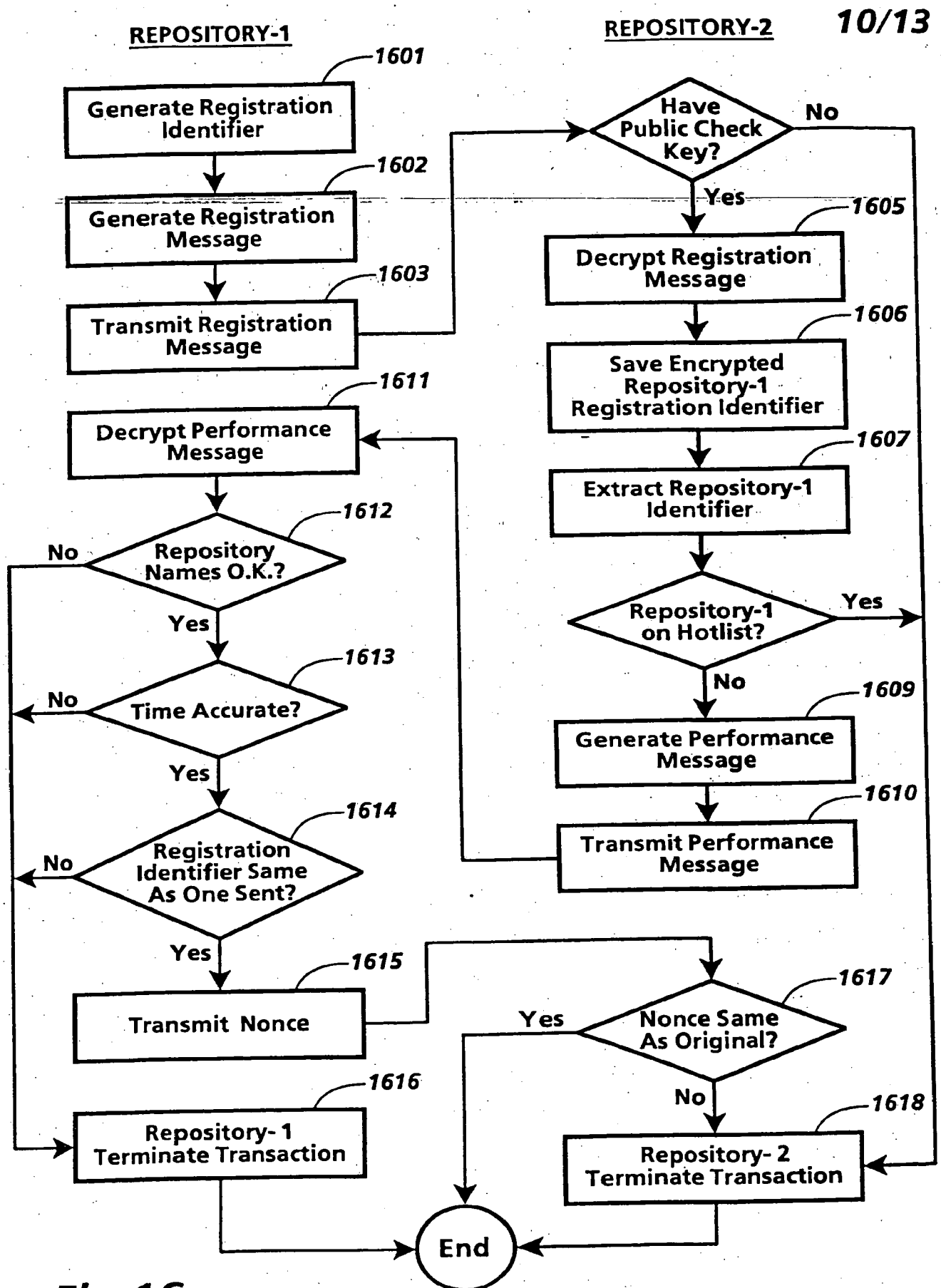
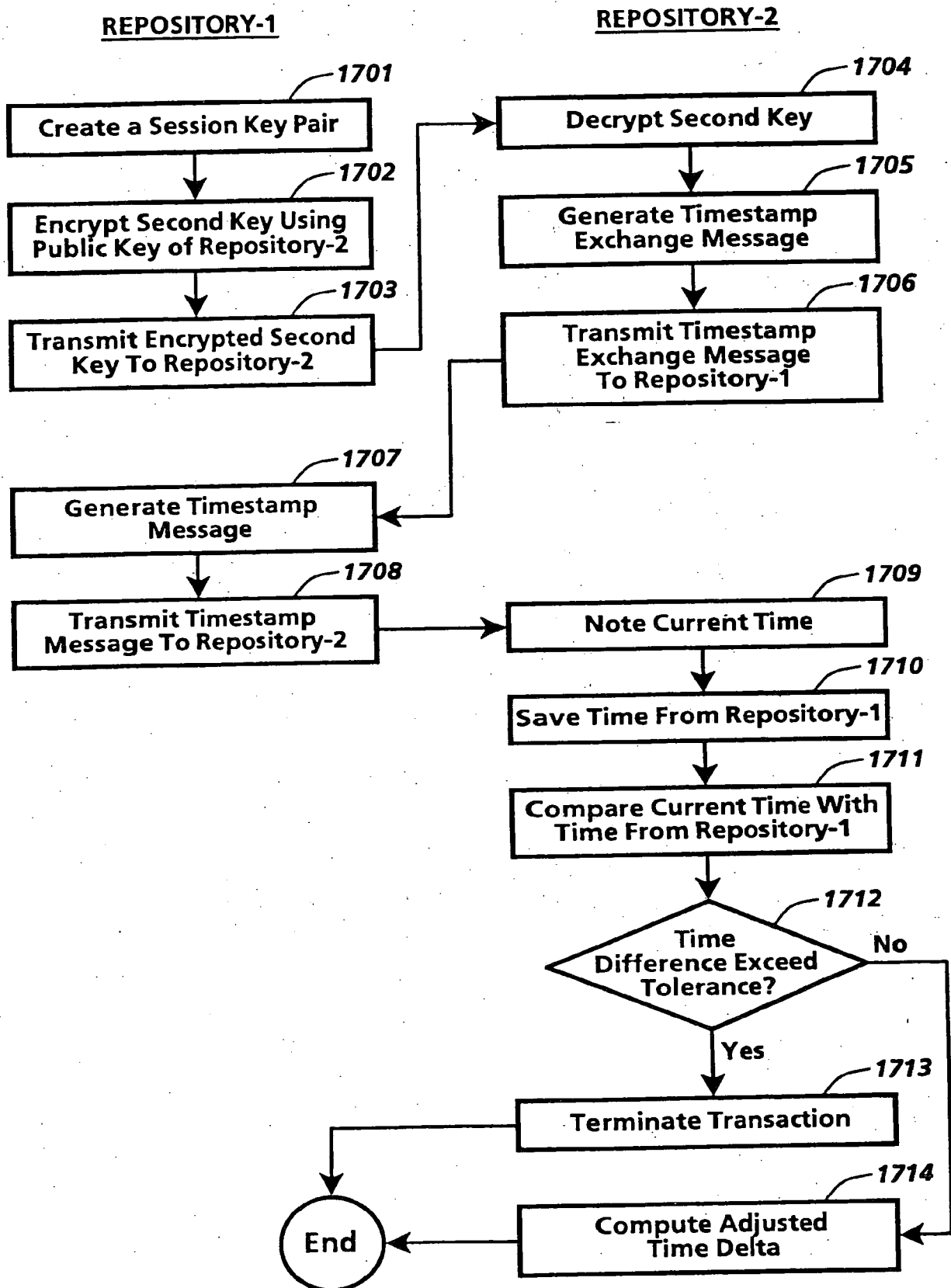
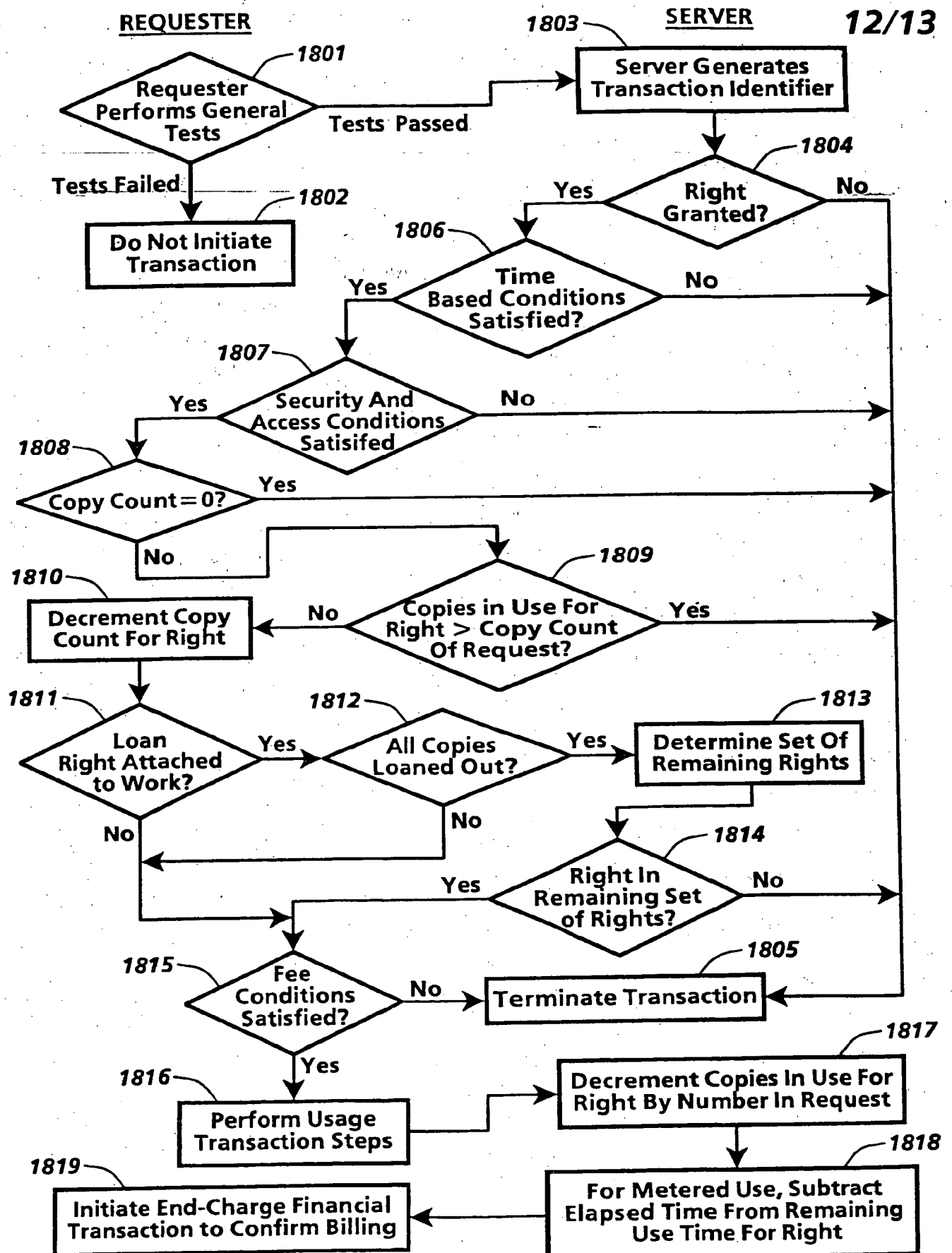
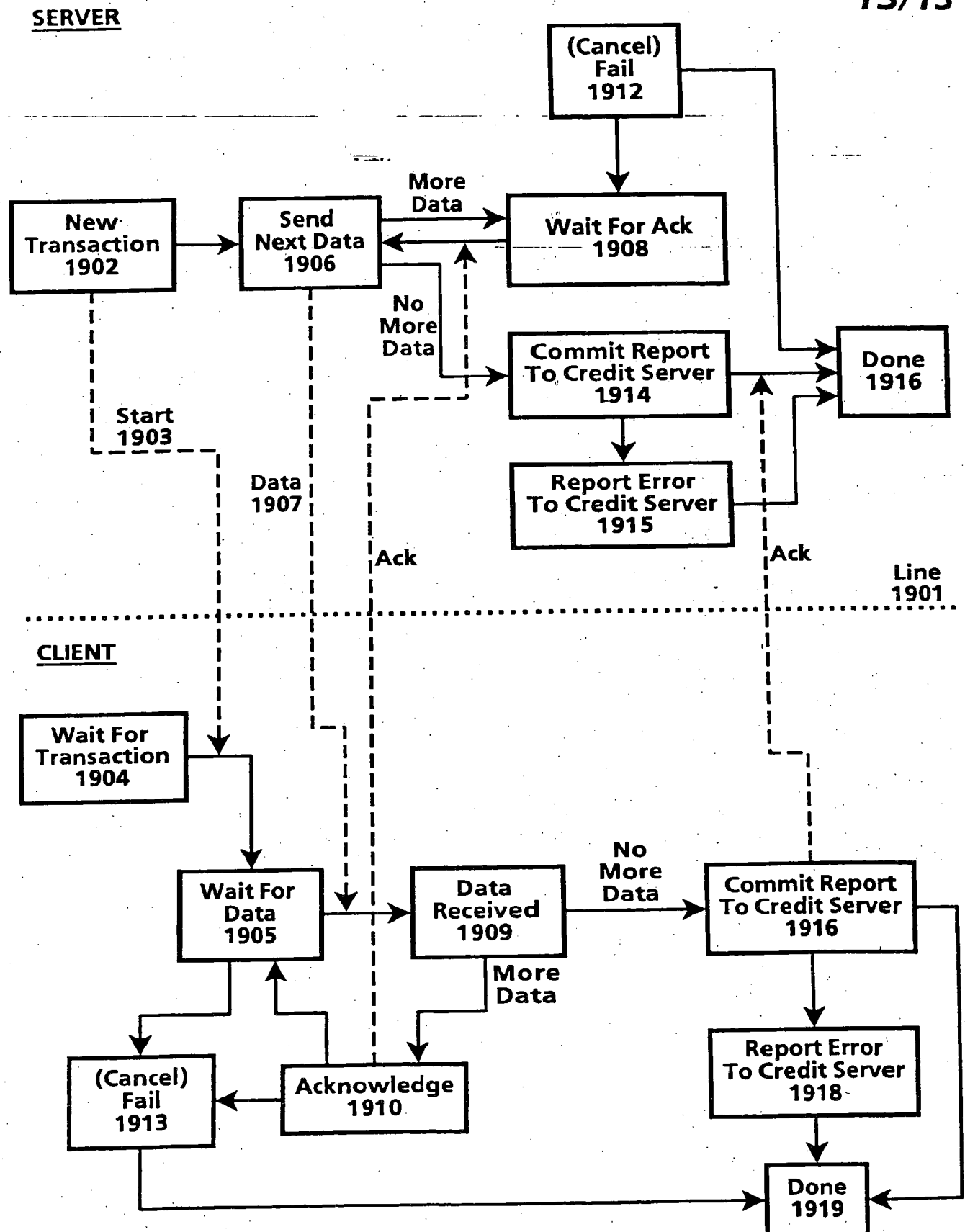


Fig.16

**Fig.17**



**Fig.19**

Electronic Patent Application Fee Transmittal				
Application Number:				
Filing Date:				
Title of Invention:		SYSTEM AND METHOD FOR DISTRIBUTING DIGITAL CONTENT TO BE RENDERED IN ACCORDANCE WITH USAGE RIGHTS INFORMATION		
First Named Inventor/Applicant Name:		Mark J. Stefik		
Filer:		Stephen M. Hertzler/Kristen Armellino		
Attorney Docket Number:		10-510-US-C73		
Filed as Large Entity				
Track I Prioritized Examination - Nonprovisional Application under 35 USC 111(a) Filing Fees				
Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Basic Filing:				
Utility application filing	1011	1	380	380
Utility Search Fee	1111	1	620	620
Utility Examination Fee	1311	1	250	250
Request for Prioritized Examination	1817	1	4800	4800
Pages:				
Claims:				
Miscellaneous-Filing:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Publ. Fee- early, voluntary, or normal	1504	1	300	300
Processing Fee, except for Provis. apps	1808	1	130	130
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				
Miscellaneous:				
Total in USD (\$)				6480

Electronic Acknowledgement Receipt

EFS ID:	13489845
Application Number:	13585408
International Application Number:	
Confirmation Number:	4941
Title of Invention:	SYSTEM AND METHOD FOR DISTRIBUTING DIGITAL CONTENT TO BE RENDERED IN ACCORDANCE WITH USAGE RIGHTS INFORMATION
First Named Inventor/Applicant Name:	Mark J. Stefik
Customer Number:	98804
Filer:	Stephen M. Hertzler
Filer Authorized By:	
Attorney Docket Number:	10-510-US-C73
Receipt Date:	14-AUG-2012
Filing Date:	
Time Stamp:	16:22:59
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Credit Card
Payment was successfully received in RAM	\$6480
RAM confirmation Number	3049
Deposit Account	501529
Authorized User	HERTZLER,STEPHEN M.

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.19 (Document supply fees)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	TrackOne Request	10-510-US-C73_-_2012-08-14_-_Track_1_Request.pdf	140815	no	2
			1465de7d91e7bc2122e3e3ba0db7d19e6911f849		
Warnings:					
Information:					
2	Application Data Sheet	10-510-US-C73_-_2012-08-14_-_Application_Data_Sheet.pdf	1094103	no	5
			a4f164722bfee6540c2882d4c1405b98b58b77d2		
Warnings:					
Information:					
3	Oath or Declaration filed	10-510-US-C73_-_2012-08-14_-_Declarations.pdf	772105	no	3
			61db68800ffd2a28b0455973665c3b80688c6a4b		
Warnings:					
Information:					
4		10-510-US-C73_-_2012-08-14_-_Specification.pdf	1099238	yes	78
			3577bda762b1c1d2d71d9eeb513927eff38efc7b		
	Multipart Description/PDF files in .zip description				
	Document Description		Start	End	
	Specification		1	73	
	Claims		74	77	
	Abstract		78	78	
Warnings:					
Information:					
5	Drawings-only black and white line drawings	10-510-US-C73_-_2012-08-14_-_Figures.pdf	3111115	no	13
			d3992023ca2f8b8e53bb66317d79319997a42899		
Warnings:					
Information:					
6	Fee Worksheet (SB06)	fee-info.pdf	40575	no	2
			1fd2f9b91d452c1b947f8c144a842944e1e06fa		
Warnings:					
Information:					
Total Files Size (in bytes):			6257951		

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 APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875						Application or Docket Number 13/585,408				
APPLICATION AS FILED - PART I										
(Column 1)		(Column 2)		SMALL ENTITY		OTHER THAN SMALL ENTITY				
FOR	NUMBER FILED	NUMBER EXTRA	RATE(\$)	FEE(\$)		RATE(\$)	FEE(\$)			
BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A			N/A	380			
SEARCH FEE (37 CFR 1.16(k), (l), or (m))	N/A	N/A	N/A			N/A	620			
EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A			N/A	250			
TOTAL CLAIMS (37 CFR 1.16(j))	15	minus 20 = *			OR	x 60 =	0.00			
INDEPENDENT CLAIMS (37 CFR 1.16(h))	3	minus 3 = *				x 250 =	0.00			
APPLICATION SIZE FEE (37 CFR 1.16(s)) If the specification and drawings exceed 100 sheets of paper, the application size fee due is \$310 (\$155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).							0.00			
							0.00			
MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))							0.00			
			TOTAL			TOTAL	1250			
* If the difference in column 1 is less than zero, enter "0" in column 2.										
APPLICATION AS AMENDED - PART II										
(Column 1)		(Column 2)		(Column 3)		SMALL ENTITY		OTHER THAN SMALL ENTITY		
AMENDMENT A		CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE(\$)	ADDITIONAL FEE(\$)	RATE(\$)	ADDITIONAL FEE(\$)	
	Total (37 CFR 1.16(i))	*	Minus	**	=	x =		OR	x =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	x =		OR	x =	
	Application Size Fee (37 CFR 1.16(s))							OR		
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	
AMENDMENT B		CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE(\$)	ADDITIONAL FEE(\$)	RATE(\$)	ADDITIONAL FEE(\$)	
	Total (37 CFR 1.16(i))	*	Minus	**	=	x =		OR	x =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	x =		OR	x =	
	Application Size Fee (37 CFR 1.16(s))							OR		
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	
* If the entry in column 1 is less than the entry in column 2, write "0" in column 3. ** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20". *** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3". The "Highest Number Previously Paid For" (Total or Independent) is the highest found in the appropriate box in column 1.										



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING or 371(c) DATE	GRP ART UNIT	FIL FEE REC'D	ATTY. DOCKET NO	TOT CLAIMS	IND CLAIMS
13/585,408	08/14/2012	2431	1550	10-510-US-C73	15	3

CONFIRMATION NO. 4941

98804
Reed Smith LLP
P.O. Box 488
Pittsburgh, PA 15230

FILING RECEIPT



Date Mailed: 08/28/2012

Receipt is acknowledged of this non-provisional patent application. The application will be taken up for examination in due course. Applicant will be notified as to the results of the examination. Any correspondence concerning the application must include the following identification information: the U.S. APPLICATION NUMBER, FILING DATE, NAME OF APPLICANT, and TITLE OF INVENTION. Fees transmitted by check or draft are subject to collection. Please verify the accuracy of the data presented on this receipt. **If an error is noted on this Filing Receipt, please submit a written request for a Filing Receipt Correction. Please provide a copy of this Filing Receipt with the changes noted thereon. If you received a "Notice to File Missing Parts" for this application, please submit any corrections to this Filing Receipt with your reply to the Notice. When the USPTO processes the reply to the Notice, the USPTO will generate another Filing Receipt incorporating the requested corrections**

Applicant(s)

Mark J. Stefik, Portola Valley, CA;
Peter L.T. Pirolli, San Francisco, CA;

Assignment For Published Patent Application

CONTENTGUARD HOLDINGS, INC., Wilmington, DE

Power of Attorney: The patent practitioners associated with Customer Number 22204

Domestic Priority data as claimed by applicant

This application is a CON of 13/584,782 08/13/2012 *
which is a CON of 11/304,793 12/16/2005
which is a DIV of 11/135,352 05/24/2005 PAT 7266529
which is a CON of 10/322,759 12/19/2002 PAT 6898576
which is a CON of 09/778,001 02/07/2001 PAT 6708157
which is a DIV of 08/967,084 11/10/1997 PAT 6236971
which is a CON of 08/344,760 11/23/1994 ABN
(*Data provided by applicant is not consistent with PTO records.

Foreign Applications (You may be eligible to benefit from the **Patent Prosecution Highway** program at the USPTO. Please see <http://www.uspto.gov> for more information.)

If Required, Foreign Filing License Granted: 08/22/2012

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 13/585,408**

Projected Publication Date: Perfected

Non-Publication Request: No

Early Publication Request: No
Title

SYSTEM AND METHOD FOR DISTRIBUTING DIGITAL CONTENT TO BE RENDERED IN
ACCORDANCE WITH USAGE RIGHTS INFORMATION

Preliminary Class

713

PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES

Since the rights granted by a U.S. patent extend only throughout the territory of the United States and have no effect in a foreign country, an inventor who wishes patent protection in another country must apply for a patent in a specific country or in regional patent offices. Applicants may wish to consider the filing of an international application under the Patent Cooperation Treaty (PCT). An international (PCT) application generally has the same effect as a regular national patent application in each PCT-member country. The PCT process **simplifies** the filing of patent applications on the same invention in member countries, but **does not result** in a grant of "an international patent" and does not eliminate the need of applicants to file additional documents and fees in countries where patent protection is desired.

Almost every country has its own patent law, and a person desiring a patent in a particular country must make an application for patent in that country in accordance with its particular laws. Since the laws of many countries differ in various respects from the patent law of the United States, applicants are advised to seek guidance from specific foreign countries to ensure that patent rights are not lost prematurely.

Applicants also are advised that in the case of inventions made in the United States, the Director of the USPTO must issue a license before applicants can apply for a patent in a foreign country. The filing of a U.S. patent application serves as a request for a foreign filing license. The application's filing receipt contains further information and guidance as to the status of applicant's license for foreign filing.

Applicants may wish to consult the USPTO booklet, "General Information Concerning Patents" (specifically, the section entitled "Treaties and Foreign Patents") for more information on timeframes and deadlines for filing foreign patent applications. The guide is available either by contacting the USPTO Contact Center at 800-786-9199, or it can be viewed on the USPTO website at <http://www.uspto.gov/web/offices/pac/doc/general/index.html>.

For information on preventing theft of your intellectual property (patents, trademarks and copyrights), you may wish to consult the U.S. Government website, <http://www.stopfakes.gov>. Part of a Department of Commerce initiative, this website includes self-help "toolkits" giving innovators guidance on how to protect intellectual property in specific countries such as China, Korea and Mexico. For questions regarding patent enforcement issues, applicants may call the U.S. Government hotline at 1-866-999-HALT (1-866-999-4158).

LICENSE FOR FOREIGN FILING UNDER
Title 35, United States Code, Section 184
Title 37, Code of Federal Regulations, 5.11 & 5.15

GRANTED

The applicant has been granted a license under 35 U.S.C. 184, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" followed by a date appears on this form. Such licenses are issued in all applications where the conditions for issuance of a license have been met, regardless of whether or not a license may be required as set forth in 37 CFR 5.15. The scope and limitations of this license are set forth in 37 CFR 5.15(a) unless an earlier license has been issued under 37 CFR 5.15(b). The license is subject to revocation upon written notification. The date indicated is the effective date of the license, unless an earlier license of similar scope has been granted under 37 CFR 5.13 or 5.14.

This license is to be retained by the licensee and may be used at any time on or after the effective date thereof unless it is revoked. This license is automatically transferred to any related applications(s) filed under 37 CFR 1.53(d). This license is not retroactive.

The grant of a license does not in any way lessen the responsibility of a licensee for the security of the subject matter as imposed by any Government contract or the provisions of existing laws relating to espionage and the national security or the export of technical data. Licensees should apprise themselves of current regulations especially with respect to certain countries, of other agencies, particularly the Office of Defense Trade Controls, Department of State (with respect to Arms, Munitions and Implements of War (22 CFR 121-128)); the Bureau of Industry and Security, Department of Commerce (15 CFR parts 730-774); the Office of Foreign AssetsControl, Department of Treasury (31 CFR Parts 500+) and the Department of Energy.

NOT GRANTED

No license under 35 U.S.C. 184 has been granted at this time, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" DOES NOT appear on this form. Applicant may still petition for a license under 37 CFR 5.12, if a license is desired before the expiration of 6 months from the filing date of the application. If 6 months has lapsed from the filing date of this application and the licensee has not received any indication of a secrecy order under 35 U.S.C. 181, the licensee may foreign file the application pursuant to 37 CFR 5.15(b).

SelectUSA

The United States represents the largest, most dynamic marketplace in the world and is an unparalleled location for business investment, innovation and commercialization of new technologies. The USA offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to encourage, facilitate, and accelerate business investment. To learn more about why the USA is the best country in the world to develop technology, manufacture products, and grow your business, visit SelectUSA.gov.

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875						Application or Docket Number 13/585,408				
APPLICATION AS FILED - PART I										
(Column 1)		(Column 2)		SMALL ENTITY		OR OTHER THAN SMALL ENTITY				
FOR	NUMBER FILED	NUMBER EXTRA	RATE(\$)	FEE(\$)		RATE(\$)	FEE(\$)			
BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A			N/A	380			
SEARCH FEE (37 CFR 1.16(k), (l), or (m))	N/A	N/A	N/A			N/A	620			
EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A			N/A	250			
TOTAL CLAIMS (37 CFR 1.16(j))	15	minus 20 = *			OR	x 60 =	0.00			
INDEPENDENT CLAIMS (37 CFR 1.16(h))	3	minus 3 = *				x 250 =	0.00			
APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is \$310 (\$155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).						0.00			
MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))							0.00			
			TOTAL			TOTAL	1250			
* If the difference in column 1 is less than zero, enter "0" in column 2.										
APPLICATION AS AMENDED - PART II										
(Column 1)		(Column 2)		(Column 3)		SMALL ENTITY		OR OTHER THAN SMALL ENTITY		
AMENDMENT A		CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE(\$)	ADDITIONAL FEE(\$)		RATE(\$)	ADDITIONAL FEE(\$)
	Total (37 CFR 1.16(i))	*	Minus	**	=	x	=	OR	x	=
	Independent (37 CFR 1.16(h))	*	Minus	***	=	x	=	OR	x	=
	Application Size Fee (37 CFR 1.16(s))							OR		
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	
AMENDMENT B		CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE(\$)	ADDITIONAL FEE(\$)		RATE(\$)	ADDITIONAL FEE(\$)
	Total (37 CFR 1.16(i))	*	Minus	**	=	x	=	OR	x	=
	Independent (37 CFR 1.16(h))	*	Minus	***	=	x	=	OR	x	=
	Application Size Fee (37 CFR 1.16(s))							OR		
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	
* If the entry in column 1 is less than the entry in column 2, write "0" in column 3. ** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20". *** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3". The "Highest Number Previously Paid For" (Total or Independent) is the highest found in the appropriate box in column 1.										



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING or 371(c) DATE	GRP ART UNIT	FIL FEE REC'D	ATTY. DOCKET NO	TOT CLAIMS	IND CLAIMS
13/585,408	08/14/2012	2431	1550	10-510-US-C73	15	3

CONFIRMATION NO. 4941

98804
Reed Smith LLP
P.O. Box 488
Pittsburgh, PA 15230

FILING RECEIPT



Date Mailed: 09/05/2012

Receipt is acknowledged of this non-provisional patent application. The application will be taken up for examination in due course. Applicant will be notified as to the results of the examination. Any correspondence concerning the application must include the following identification information: the U.S. APPLICATION NUMBER, FILING DATE, NAME OF APPLICANT, and TITLE OF INVENTION. Fees transmitted by check or draft are subject to collection. Please verify the accuracy of the data presented on this receipt. **If an error is noted on this Filing Receipt, please submit a written request for a Filing Receipt Correction. Please provide a copy of this Filing Receipt with the changes noted thereon. If you received a "Notice to File Missing Parts" for this application, please submit any corrections to this Filing Receipt with your reply to the Notice. When the USPTO processes the reply to the Notice, the USPTO will generate another Filing Receipt incorporating the requested corrections**

Applicant(s)

Mark J. Stefik, Portola Valley, CA;
Peter L.T. Pirolli, San Francisco, CA;

Assignment For Published Patent Application

CONTENTGUARD HOLDINGS, INC., Wilmington, DE

Power of Attorney: The patent practitioners associated with Customer Number 22204

Domestic Priority data as claimed by applicant

This application is a CON of 13/584,782 08/13/2012 *
which is a CON of 11/304,793 12/16/2005
which is a DIV of 11/135,352 05/24/2005 PAT 7266529
which is a CON of 10/322,759 12/19/2002 PAT 6898576
which is a CON of 09/778,001 02/07/2001 PAT 6708157
which is a DIV of 08/967,084 11/10/1997 PAT 6236971
which is a CON of 08/344,760 11/23/1994 ABN
(*Data provided by applicant is not consistent with PTO records.

Foreign Applications (You may be eligible to benefit from the **Patent Prosecution Highway** program at the USPTO. Please see <http://www.uspto.gov> for more information.)

If Required, Foreign Filing License Granted: 08/22/2012

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 13/585,408**

Projected Publication Date: 12/13/2012

Non-Publication Request: No

Early Publication Request: No
Title

SYSTEM AND METHOD FOR DISTRIBUTING DIGITAL CONTENT TO BE RENDERED IN
ACCORDANCE WITH USAGE RIGHTS INFORMATION

Preliminary Class

713

PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES

Since the rights granted by a U.S. patent extend only throughout the territory of the United States and have no effect in a foreign country, an inventor who wishes patent protection in another country must apply for a patent in a specific country or in regional patent offices. Applicants may wish to consider the filing of an international application under the Patent Cooperation Treaty (PCT). An international (PCT) application generally has the same effect as a regular national patent application in each PCT-member country. The PCT process **simplifies** the filing of patent applications on the same invention in member countries, but **does not result** in a grant of "an international patent" and does not eliminate the need of applicants to file additional documents and fees in countries where patent protection is desired.

Almost every country has its own patent law, and a person desiring a patent in a particular country must make an application for patent in that country in accordance with its particular laws. Since the laws of many countries differ in various respects from the patent law of the United States, applicants are advised to seek guidance from specific foreign countries to ensure that patent rights are not lost prematurely.

Applicants also are advised that in the case of inventions made in the United States, the Director of the USPTO must issue a license before applicants can apply for a patent in a foreign country. The filing of a U.S. patent application serves as a request for a foreign filing license. The application's filing receipt contains further information and guidance as to the status of applicant's license for foreign filing.

Applicants may wish to consult the USPTO booklet, "General Information Concerning Patents" (specifically, the section entitled "Treaties and Foreign Patents") for more information on timeframes and deadlines for filing foreign patent applications. The guide is available either by contacting the USPTO Contact Center at 800-786-9199, or it can be viewed on the USPTO website at <http://www.uspto.gov/web/offices/pac/doc/general/index.html>.

For information on preventing theft of your intellectual property (patents, trademarks and copyrights), you may wish to consult the U.S. Government website, <http://www.stopfakes.gov>. Part of a Department of Commerce initiative, this website includes self-help "toolkits" giving innovators guidance on how to protect intellectual property in specific countries such as China, Korea and Mexico. For questions regarding patent enforcement issues, applicants may call the U.S. Government hotline at 1-866-999-HALT (1-866-999-4158).

LICENSE FOR FOREIGN FILING UNDER
Title 35, United States Code, Section 184
Title 37, Code of Federal Regulations, 5.11 & 5.15

GRANTED

The applicant has been granted a license under 35 U.S.C. 184, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" followed by a date appears on this form. Such licenses are issued in all applications where the conditions for issuance of a license have been met, regardless of whether or not a license may be required as set forth in 37 CFR 5.15. The scope and limitations of this license are set forth in 37 CFR 5.15(a) unless an earlier license has been issued under 37 CFR 5.15(b). The license is subject to revocation upon written notification. The date indicated is the effective date of the license, unless an earlier license of similar scope has been granted under 37 CFR 5.13 or 5.14.

This license is to be retained by the licensee and may be used at any time on or after the effective date thereof unless it is revoked. This license is automatically transferred to any related applications(s) filed under 37 CFR 1.53(d). This license is not retroactive.

The grant of a license does not in any way lessen the responsibility of a licensee for the security of the subject matter as imposed by any Government contract or the provisions of existing laws relating to espionage and the national security or the export of technical data. Licensees should apprise themselves of current regulations especially with respect to certain countries, of other agencies, particularly the Office of Defense Trade Controls, Department of State (with respect to Arms, Munitions and Implements of War (22 CFR 121-128)); the Bureau of Industry and Security, Department of Commerce (15 CFR parts 730-774); the Office of Foreign AssetsControl, Department of Treasury (31 CFR Parts 500+) and the Department of Energy.

NOT GRANTED

No license under 35 U.S.C. 184 has been granted at this time, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" DOES NOT appear on this form. Applicant may still petition for a license under 37 CFR 5.12, if a license is desired before the expiration of 6 months from the filing date of the application. If 6 months has lapsed from the filing date of this application and the licensee has not received any indication of a secrecy order under 35 U.S.C. 181, the licensee may foreign file the application pursuant to 37 CFR 5.15(b).

SelectUSA

The United States represents the largest, most dynamic marketplace in the world and is an unparalleled location for business investment, innovation and commercialization of new technologies. The USA offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to encourage, facilitate, and accelerate business investment. To learn more about why the USA is the best country in the world to develop technology, manufacture products, and grow your business, visit SelectUSA.gov.



UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

Reed Smith LLP
P.O. Box 488
Pittsburgh PA 15230

MAILED
SEP 06 2012
OFFICE OF PETITIONS

Doc Code: TRACK1.GRANT

Decision Granting Request for Prioritized Examination (Track I or After RCE)	Application No.: 13/585,408
1. THE REQUEST FILED <u>August 14, 2012</u> IS GRANTED. The above-identified application has met the requirements for prioritized examination A. ☒ for an original nonprovisional application (Track I). B. ☐ for an application undergoing continued examination (RCE). 2. The above-identified application will undergo prioritized examination. The application will be accorded special status throughout its entire course of prosecution until one of the following occurs: A. filing a <u>petition for extension of time</u> to extend the time period for filing a reply; B. filing an <u>amendment to amend the application to contain more than four independent claims, more than thirty total claims</u>, or a multiple dependent claim; C. filing a <u>request for continued examination</u>; D. filing a notice of appeal; E. filing a request for suspension of action; F. mailing of a notice of allowance; G. mailing of a final Office action; H. completion of examination as defined in 37 CFR 41.102; or I. abandonment of the application. Telephone inquiries with regard to this decision should be directed to Kimberly Inabinet at 571-272-4618. In his/her absence, calls may be directed to Brian W. Brown at 571-272-5338. / Kimberly A. Inabinet/ [Signature] Petitions Examiner, Office of Petitions (Title)	

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:	)	Confirmation No. 4941
Mark J. Stefik, et al.	)	Group Art Unit: 2431
Serial No. 13/585,408	)	Examiner: TBD
Filed: August 14, 2012	)	
For: SYSTEM AND METHOD FOR	)	
DISTRIBUTING DIGITAL CONTENT	)	
TO BE RENDERED IN ACCORDANCE	)	
WITH USAGE RIGHTS	)	
INFORMATION	)	

SUBMISSION OF REPLACEMENT DRAWINGS

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

Applicants submits herewith replacement drawing figures 1-19 in compliance with 37 CFR 1.84 and 37 CFR 1.121(d).

The Commissioner is hereby authorized to charge fees and credit overpayments to Deposit Account No. 50-1529.

If any further information is needed, please contact the undersigned.

Date: September 11, 2012

Respectfully submitted,

/Stephen M. Hertzler, Reg. No. 58,247/

Stephen M. Hertzler
Registration No. 58,247

REED SMITH LLP
CUSTOMER NO.: 98804
1301 K Street N.W.
Suite 1100 – East Tower
Washington, D.C. 20005

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:	)	Confirmation No. 4941
Mark J. Stefik, et al.	)	Group Art Unit: 2431
Serial No. 13/585,408	)	Examiner: TBD
Filed: August 14, 2012	)	
For: SYSTEM AND METHOD FOR	)	
DISTRIBUTING DIGITAL CONTENT	)	
TO BE RENDERED IN ACCORDANCE	)	
WITH USAGE RIGHTS	)	
INFORMATION	)	

SUBMISSION OF REPLACEMENT DRAWINGS

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

Applicants submits herewith replacement drawing figures 1-19 in compliance with 37 CFR 1.84 and 37 CFR 1.121(d).

The Commissioner is hereby authorized to charge fees and credit overpayments to Deposit Account No. 50-1529.

If any further information is needed, please contact the undersigned.

Date: September 11, 2012

Respectfully submitted,

/Stephen M. Hertzler, Reg. No. 58,247/

Stephen M. Hertzler
Registration No. 58,247

REED SMITH LLP
CUSTOMER NO.: 98804
1301 K Street N.W.
Suite 1100 – East Tower
Washington, D.C. 20005

FIG. 1

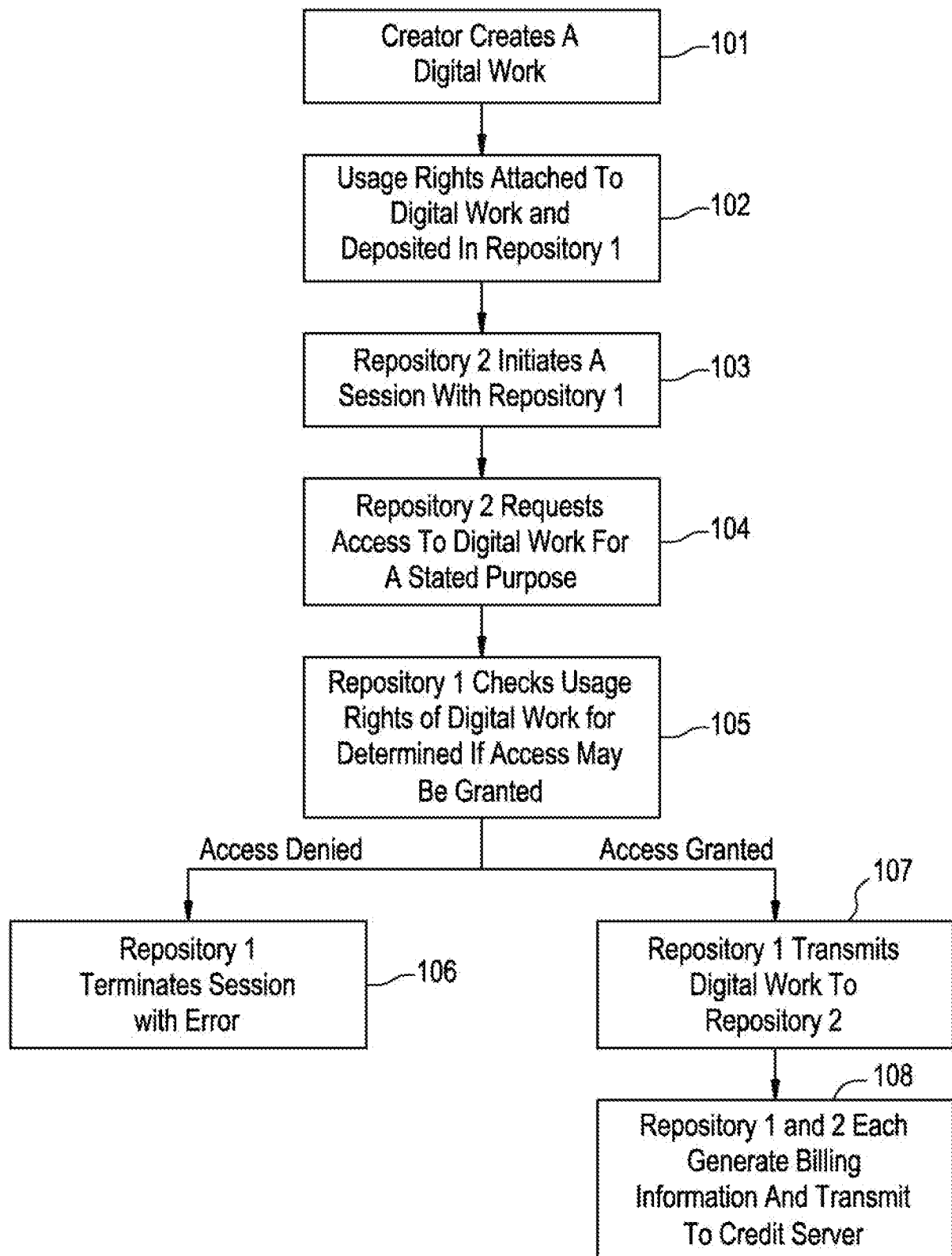


FIG. 2

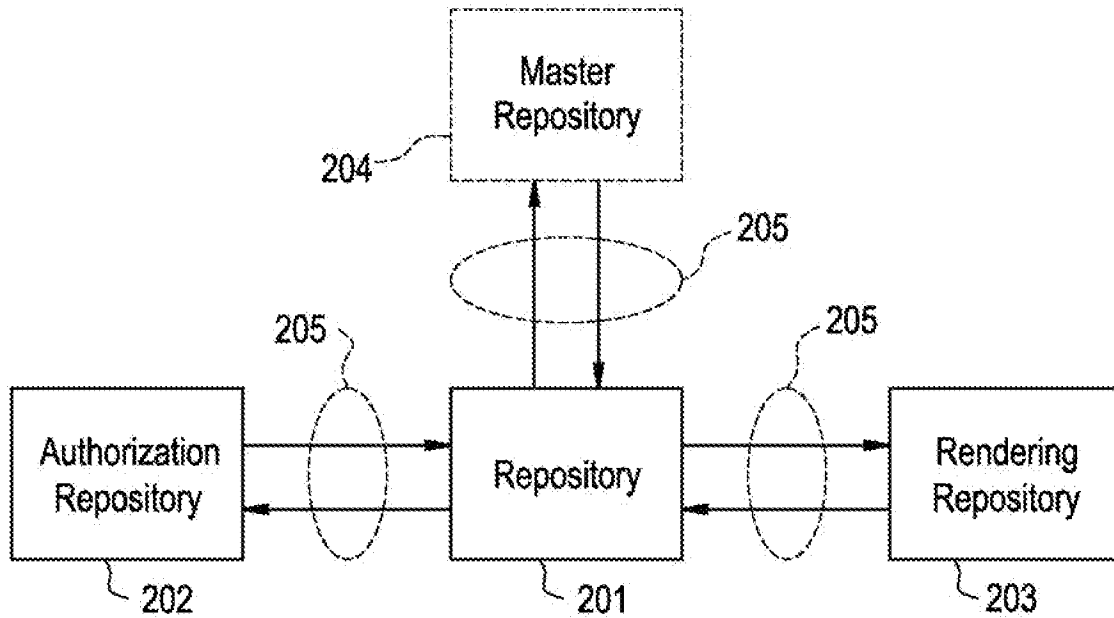


FIG. 3

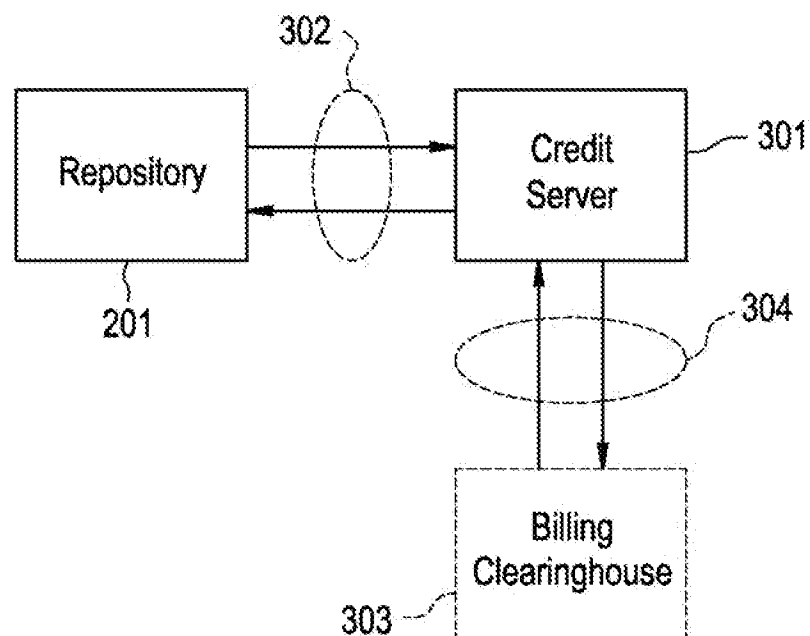


FIG. 4A

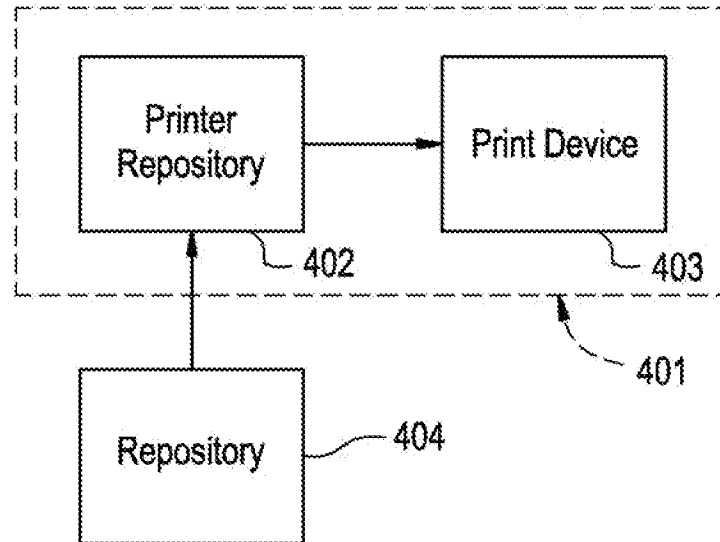


FIG. 4B

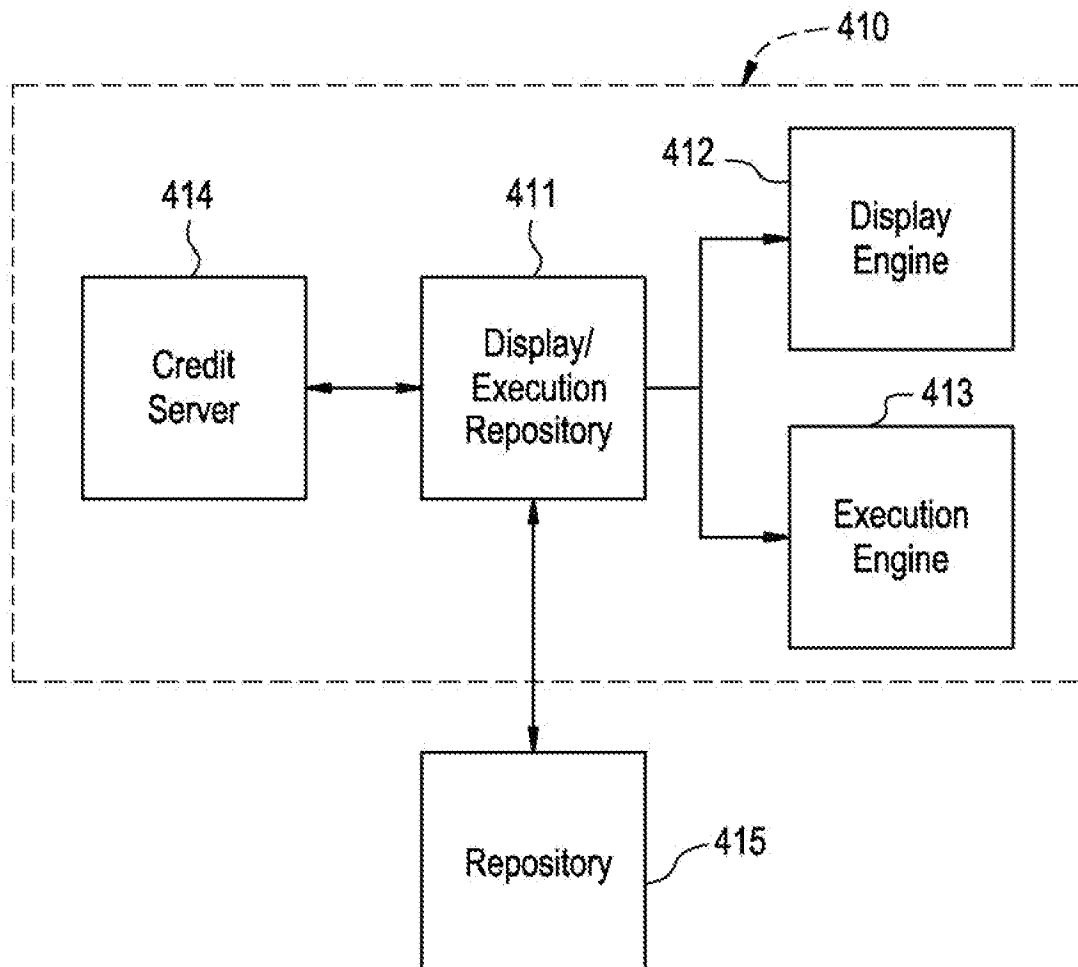


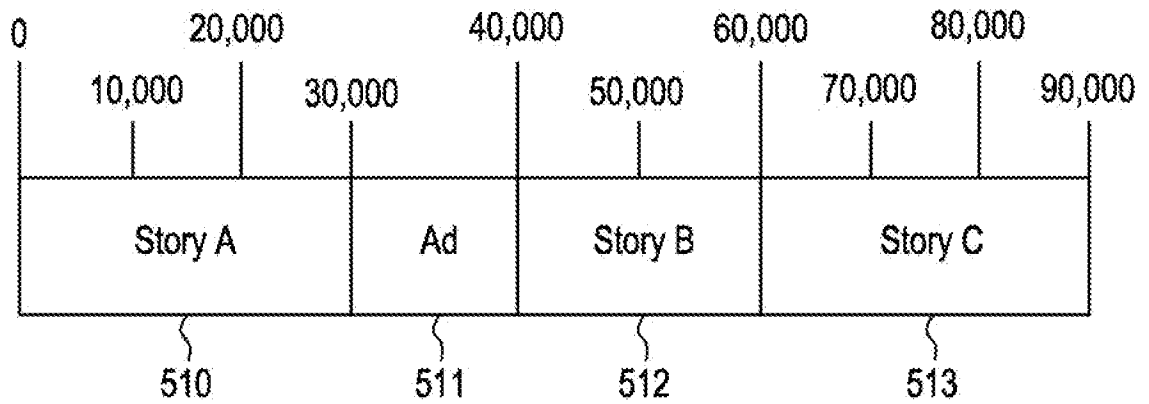
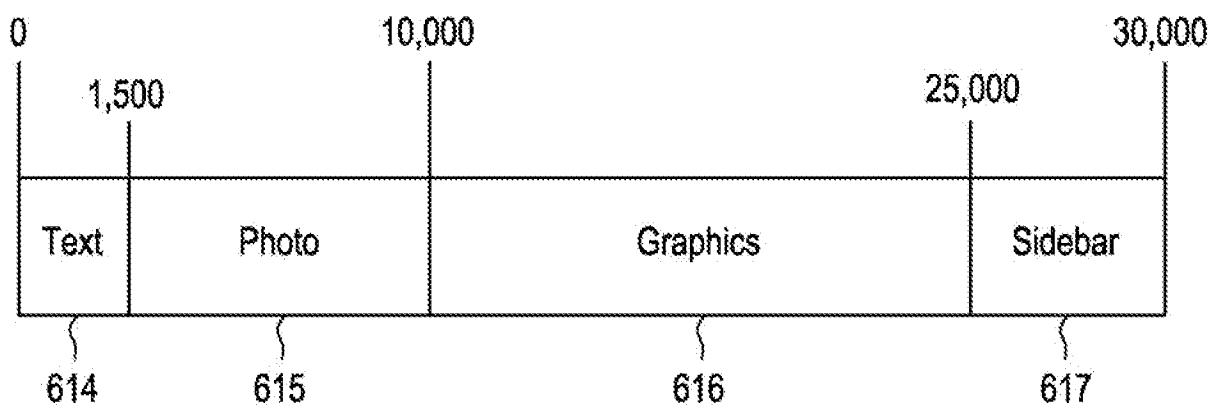
FIG. 5**FIG. 6**

FIG. 7

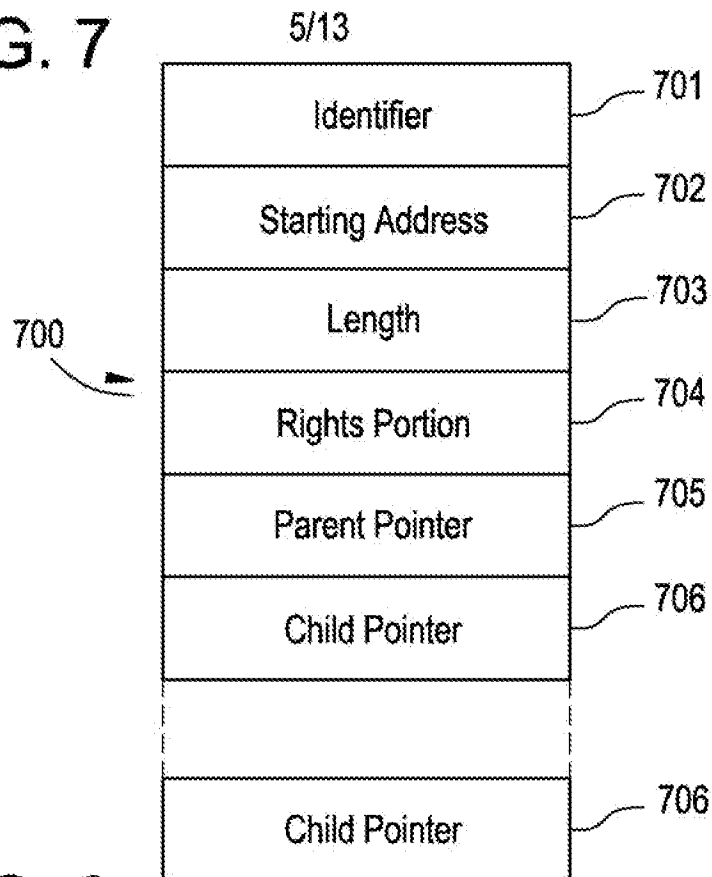


FIG. 8

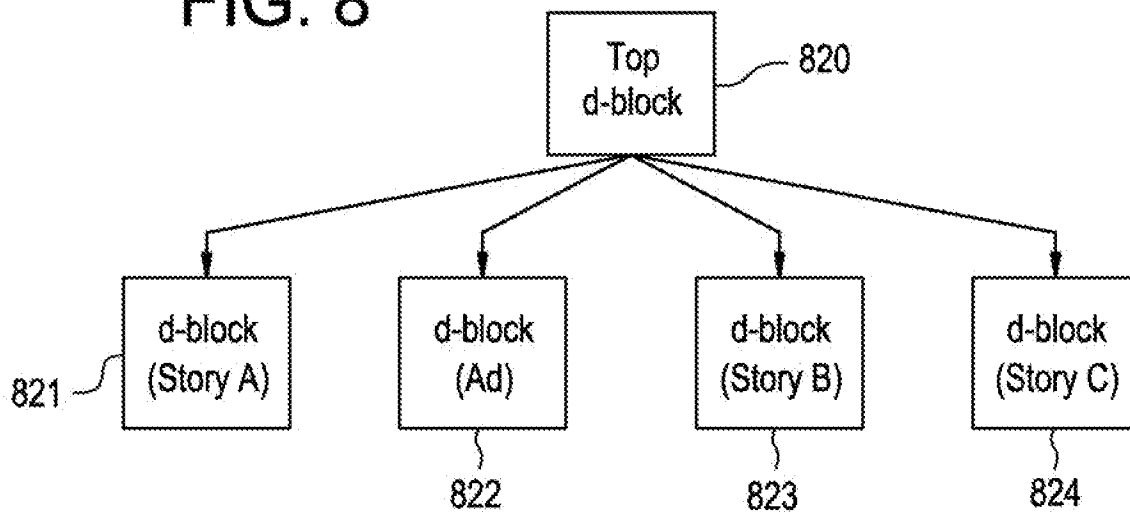


FIG. 9

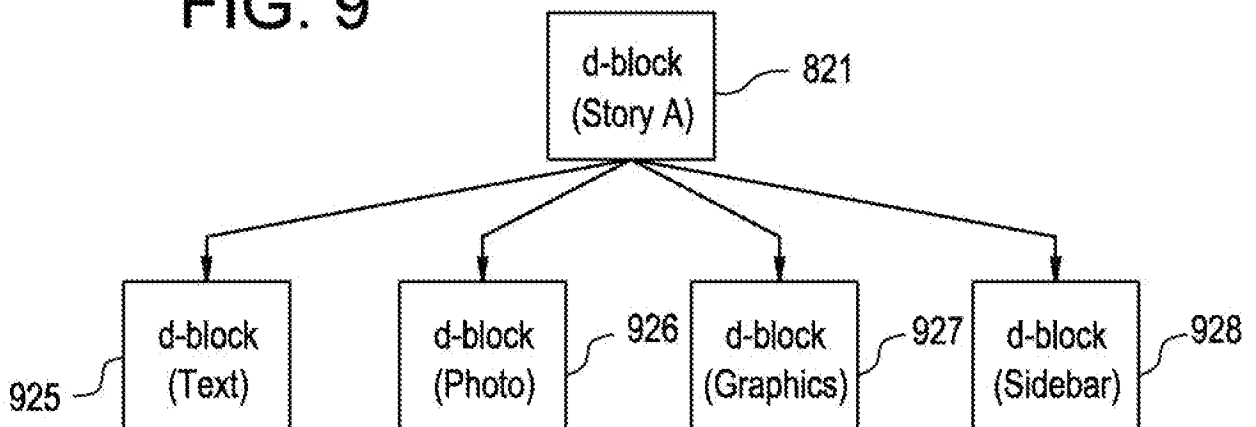


FIG. 10

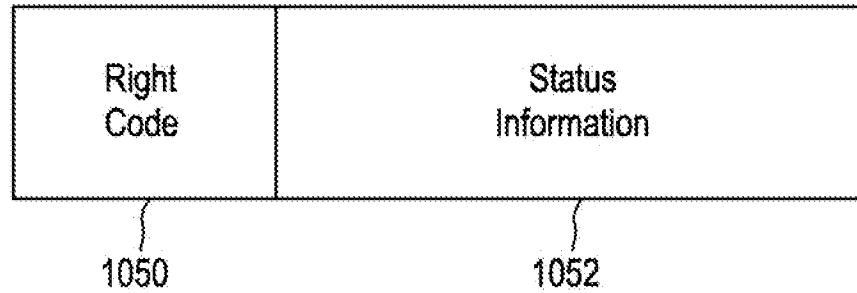


FIG. 14

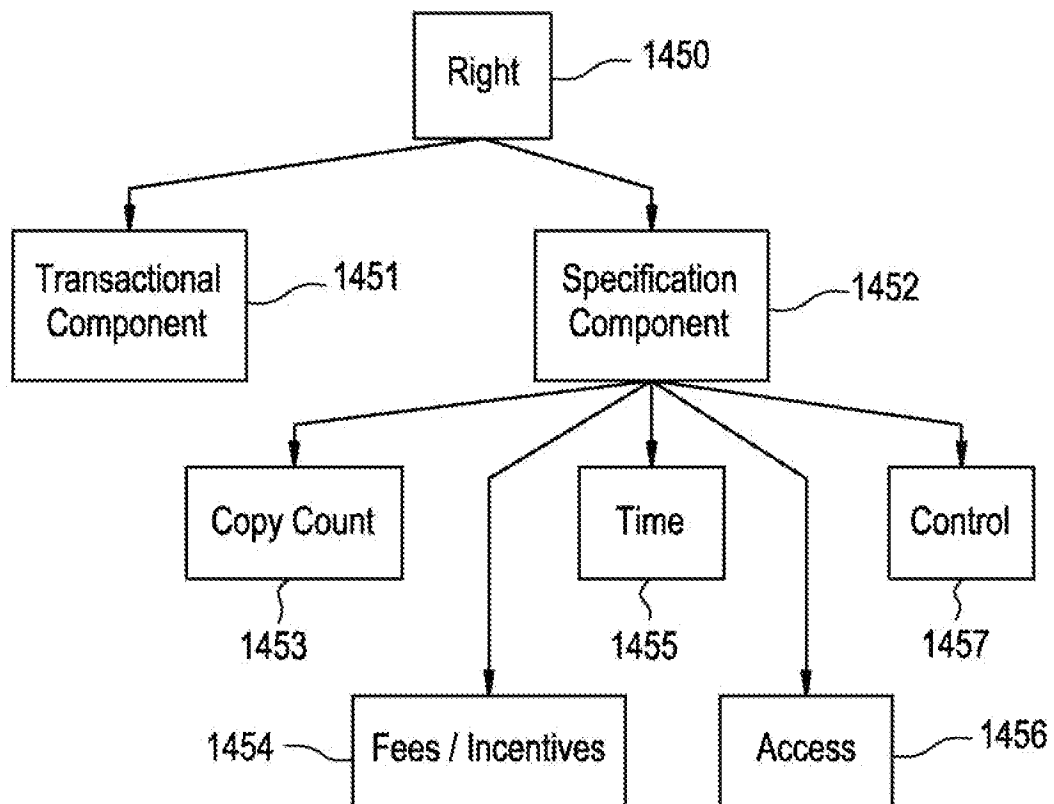


FIG. 11

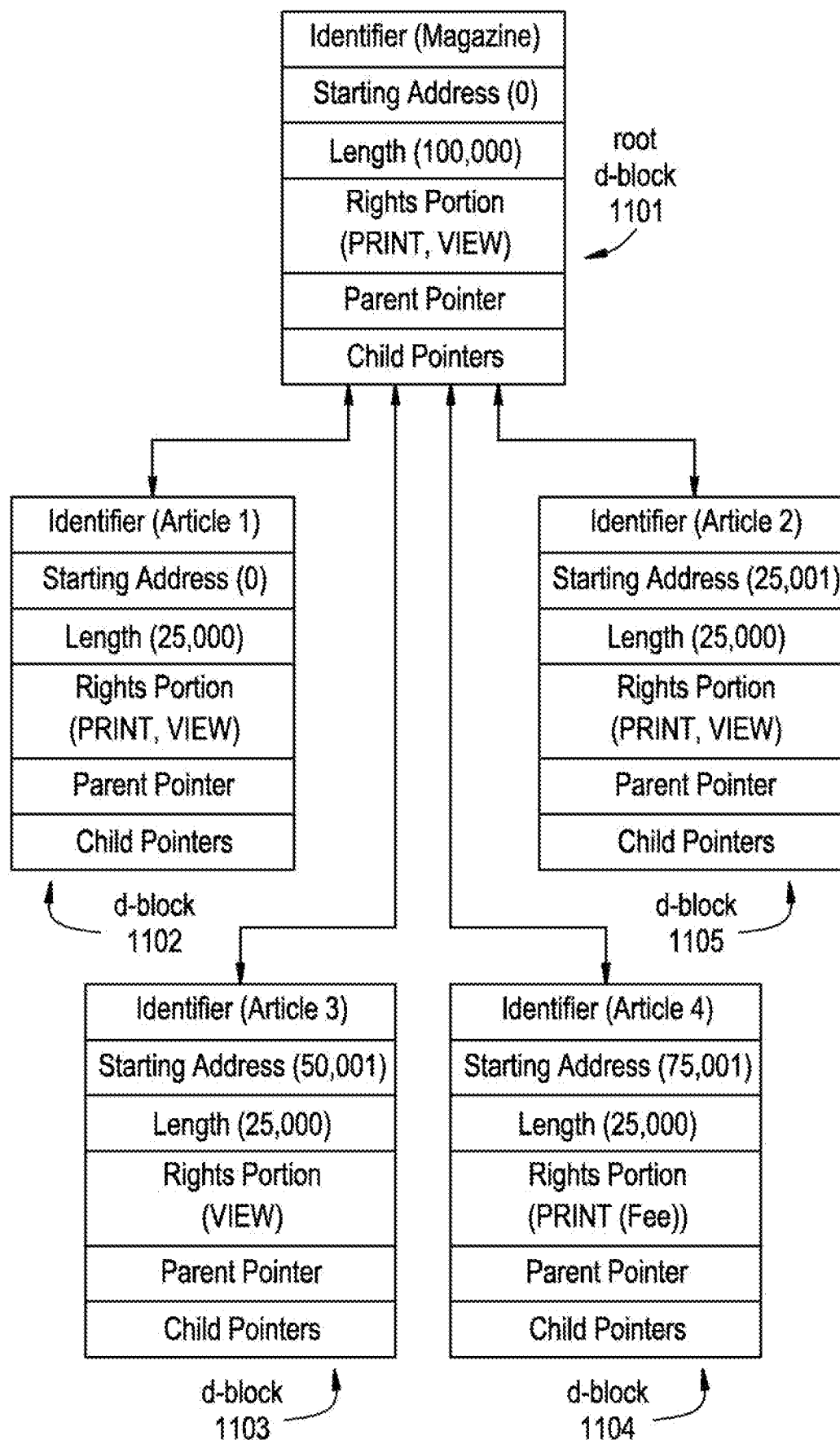


FIG. 12

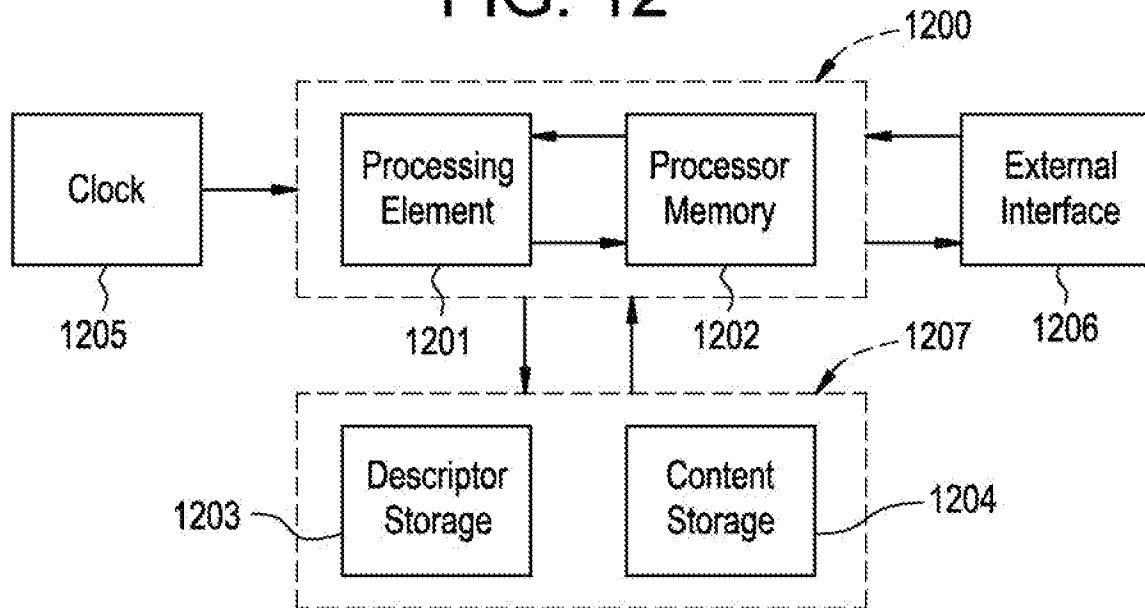


FIG. 13

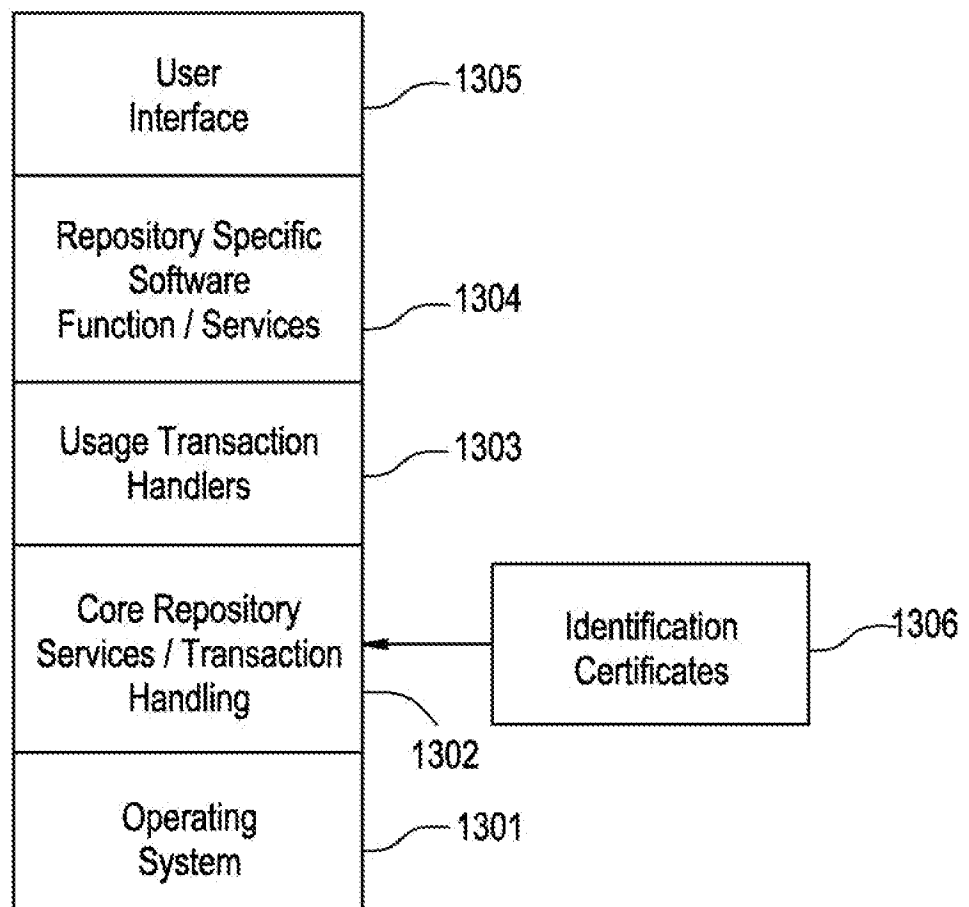


FIG. 15

9/13

- 1501 — Digital Work Rights: = (Rights*)
- 1502 — Right: = (Right-Code {Copy-Count} {Control-Spec} {Time-Spec}
{Access-Spec} {Fee-Spec})
- 1503 — Right-Code: = Render-Code | Transport-Code | File-Management-
Code | Derivative-Works-Code | Configuration-Code
- 1504 — Render-Code: = [Play: {Player: Player-ID} | Print: {Printer: Printer-ID}]
- 1505 — Transport-Code: = [Copy | Transfer | Loan {Remaining-Rights:
Next-Set-of-Rights}] {(Next-Copy-Rights: Next-Set-of-Rights)}
- 1506 — File-Management-Code: = Backup {Back-Up-Copy-Rights:
Next-Set-of-Rights} | Restore | Delete | Folder
| Directory {Name: Hide-Local | Hide-Remote}
{Parts: Hide-Local | Hide-Remote}
- 1507 — Derivative-Works-Code: = [Extract | Embed | Edit {Process:
Process-ID}] {(Next-Copy-Rights:
Next-Set-of-Rights)}
- 1508 — Configuration-Code: = Install | Uninstall
- 1509 — Next-Set-of-Rights: = {(Add: Set-of-Rights)} {(Delete:
Set-of-Rights)} {(Replace: Set-of-Rights)} {(Keep: Set-of-Rights)}
- 1510 — Copy-Count: = (Copies: positive-integer | 0 | Unlimited)
- 1511 — Control-Spec: = (Control: {Restrictable | Unrestrictable}
{Unchargeable | Chargeable})
- 1512 — Time-Spec: = {(Fixed-Interval | Sliding-Interval | Meter-Time)
Until: Expiration-Date}
- 1513 — Fixed-Interval: = From: Start-Time
- 1514 — Sliding-Interval: = Interval : Use-Duration
- 1515 — Meter-Time: = Time-Remaining: Remaining-Use
- 1516 — Access-Spec: = {(SC: Security-Class} {Authorization: Authorization-ID*}
{Other-Authorization: Authorization-ID*} {Ticket: Ticket-ID})
- 1517 — Fee-Spec: = {Scheduled-Discount} Regular-Fee-Spec | Scheduled-Fee-Spec |
Markup-Spec
- 1518 — Scheduled-Discount: = Scheduled-Discount: (Scheduled-Discount:
(Time-Spec Percentage)*)
- 1519 — Regular-Fee-Spec: = {(Fee: | Incentive:) [Per-Use-Spec | Metered-Rate-
Spec | Best-Price-Spec | Call-For-Price-Spec]
{Min: Money-Unit Per: Time-Spec} {Max:
Money-Unit Per: Time-Spec} To: Account-ID}
- 1520 — Per-Use-Spec: = Per-Use: Money-Unit
- 1521 — Metered-Rate-Spec: = Metered: Money-Unit Per: Time-Spec
- 1522 — Best-Price-Spec: = Best-Price: Money-unit Max: Money-Unit
- 1523 — Call-For-Price-Spec: = Call-For-Price
- 1524 — Scheduled-Fee-Spec: = (Schedule: (Time-Spec Regular-Fee-Spec)*)
- 1525 — Markup-Spec: = Markup: percentage To: Account-ID

FIG. 16

10/13

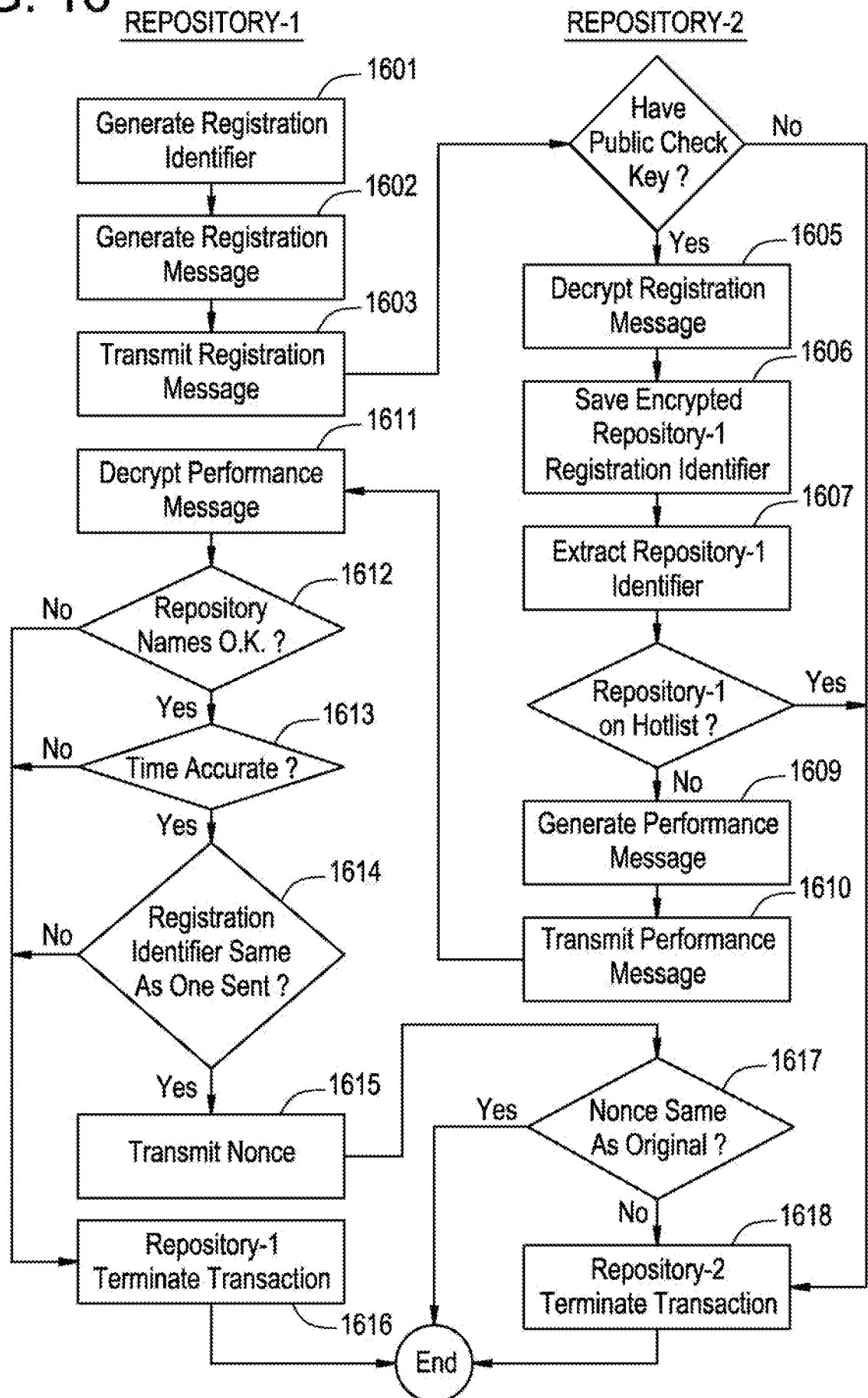


FIG. 17

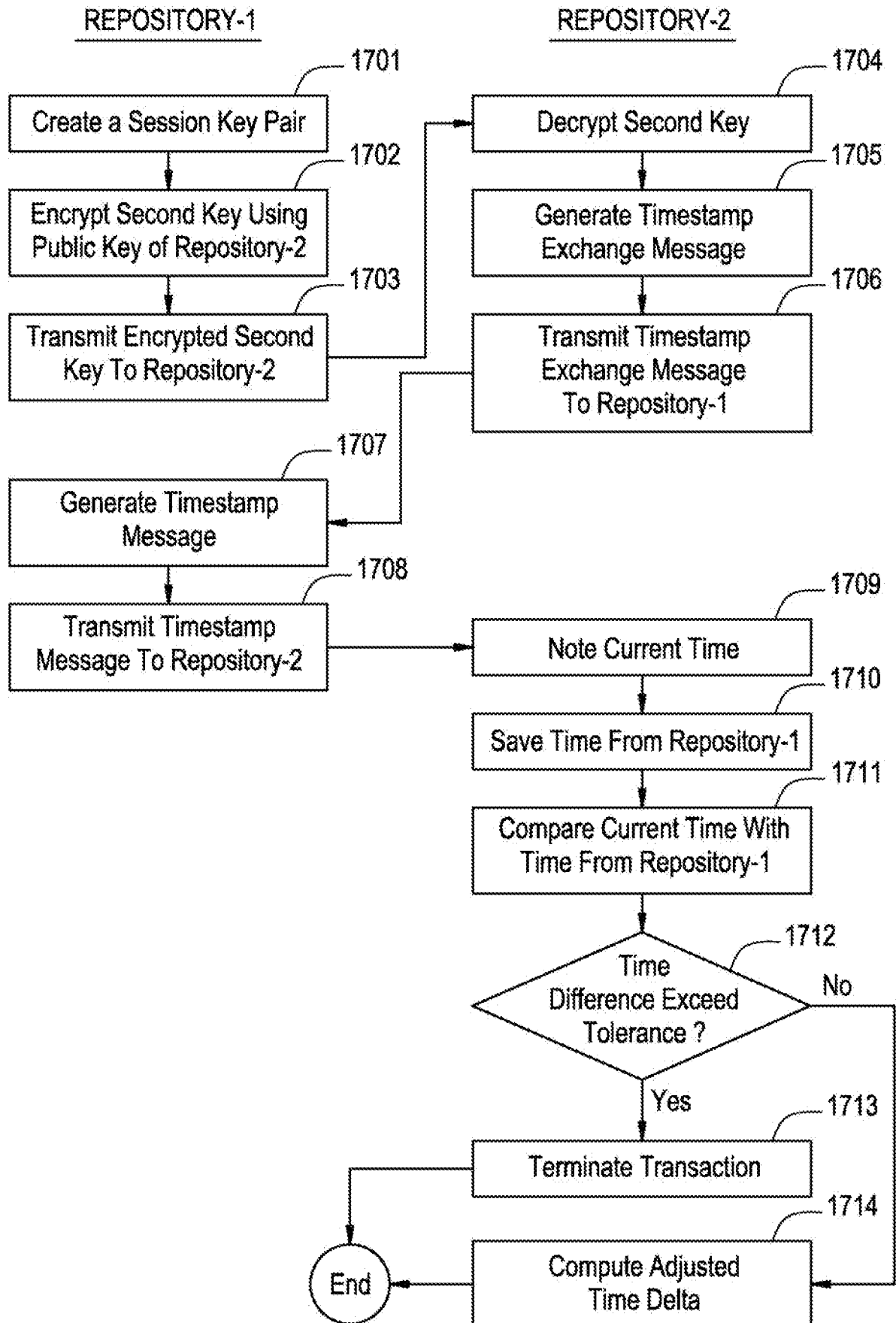


FIG. 18

12/13

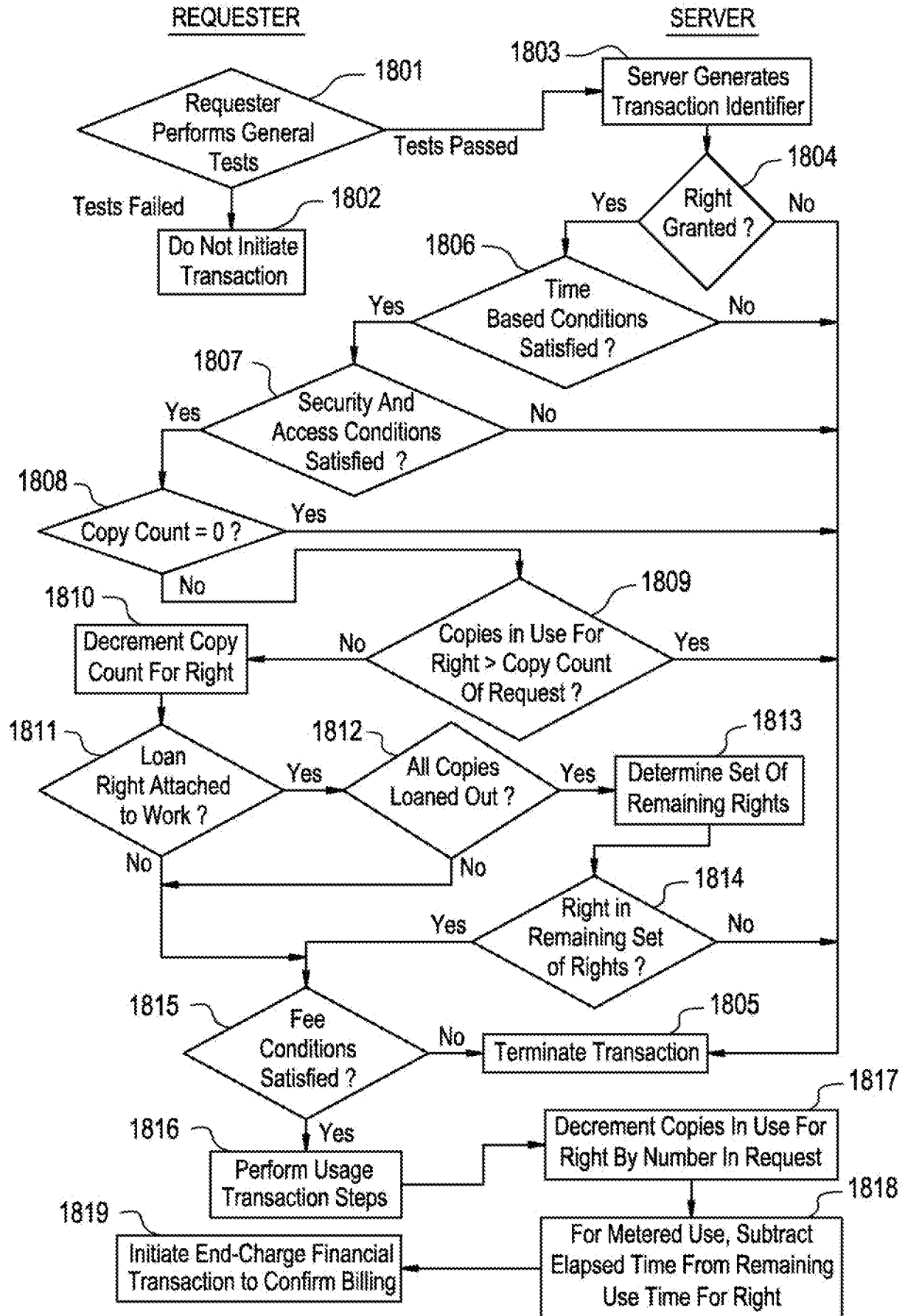
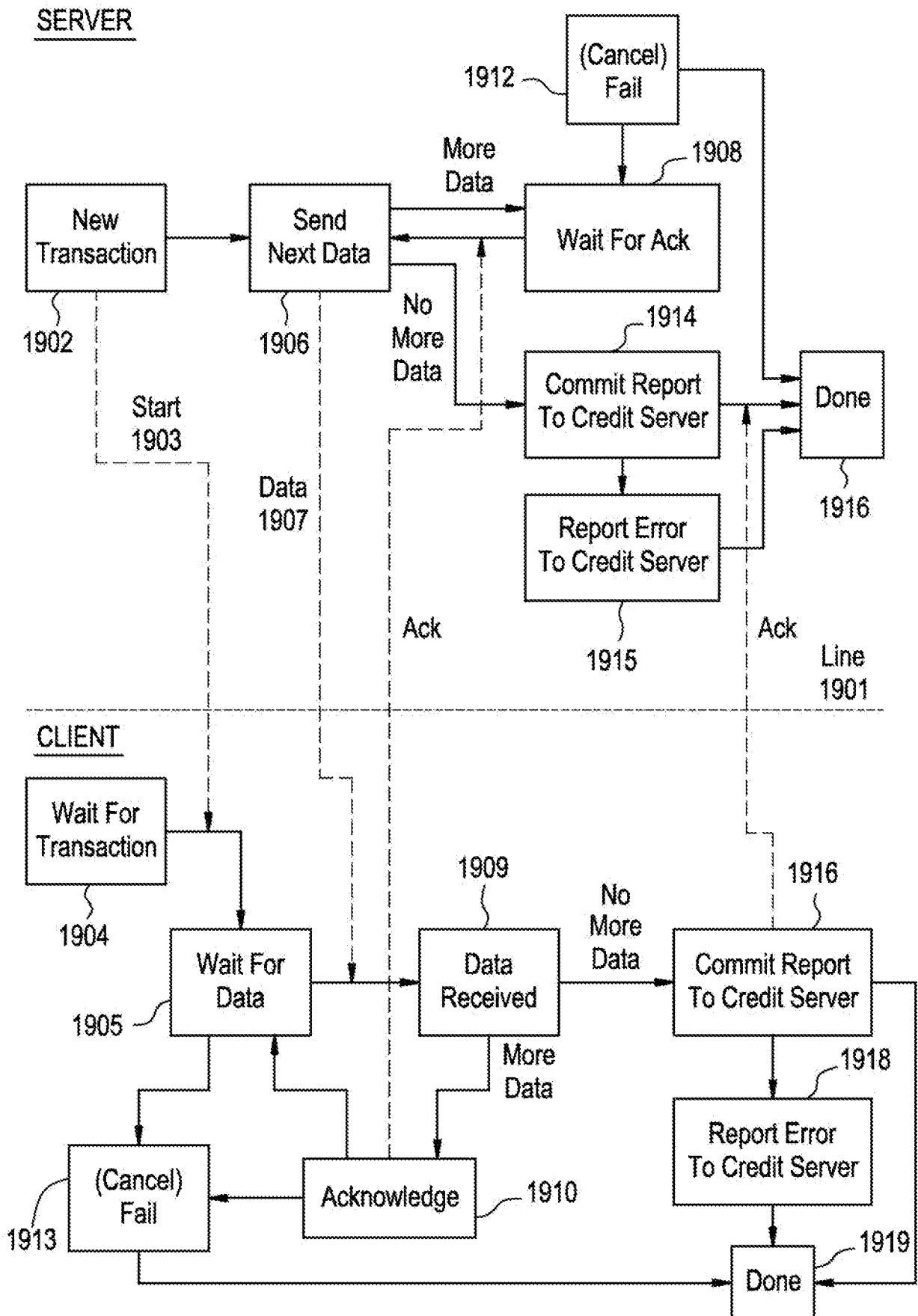


FIG. 19



Electronic Acknowledgement Receipt

EFS ID:	13712246
Application Number:	13585408
International Application Number:	
Confirmation Number:	4941
Title of Invention:	SYSTEM AND METHOD FOR DISTRIBUTING DIGITAL CONTENT TO BE RENDERED IN ACCORDANCE WITH USAGE RIGHTS INFORMATION
First Named Inventor/Applicant Name:	Mark J. Stefik
Customer Number:	98804
Filer:	Stephen M. Hertzler
Filer Authorized By:	
Attorney Docket Number:	10-510-US-C73
Receipt Date:	11-SEP-2012
Filing Date:	14-AUG-2012
Time Stamp:	16:28:54
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	Transmittal Letter	10-510-US-C73_Transmittal_Replacement_Drawings.pdf	475218 15ed5dbffc38c3e2036cf8e2ab83c2d1c1cf0210	no	1

Warnings:

Information:

2	Drawings-only black and white line drawings	10-510-US-C73_Replacement_Drawings.pdf	1731664 29c459bc5a1d731c25239d4d5d43e1dc0fe0adf0	no	13
Warnings:					
Information:					
Total Files Size (in bytes):			2206882		
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. <u>New Applications Under 35 U.S.C. 111</u> 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. <u>National Stage of an International Application under 35 U.S.C. 371</u> 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. <u>New International Application Filed with the USPTO as a Receiving Office</u> 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.					

POWER OF ATTORNEY TO PROSECUTE APPLICATIONS BEFORE THE USPTO

I hereby revoke all previous powers of attorney given in the application identified in the attached statement under 37 CFR 3.73(b).

I hereby appoint:



Practitioners associated with the Customer Number:

98804

OR



Practitioner(s) named below (if more than ten patent practitioners are to be named, then a customer number must be used):

Name	Registration Number	Name	Registration Number

as attorney(s) or agent(s) to represent the undersigned before the United States Patent and Trademark Office (USPTO) in connection with any and all patent applications assigned only to the undersigned according to the USPTO assignment records or assignment documents attached to this form in accordance with 37 CFR 3.73(b).

Please change the correspondence address for the application identified in the attached statement under 37 CFR 3.73(b) to:



The address associated with Customer Number:

98804

OR

☐ Firm or Individual Name			
Address			
City	State	Zip	
Country			
Telephone	Email		

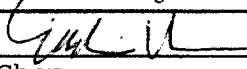
Assignee Name and Address:

ContentGuard Holdings, Inc.
222 N. Sepulveda Blvd., Suite 1400
El Segundo, CA 90245

A copy of this form, together with a statement under 37 CFR 3.73(b) (Form PTO/SB/96 or equivalent) is required to be filed in each application in which this form is used. The statement under 37 CFR 3.73(b) may be completed by one of the practitioners appointed in this form if the appointed practitioner is authorized to act on behalf of the assignee, and must identify the application in which this Power of Attorney is to be filed.

SIGNATURE of Assignee of Record

The individual whose signature and title is supplied below is authorized to act on behalf of the assignee

Signature		Date	9/16/2010
Name	Eddie Chen	Telephone	
Title	Chief Technology Officer		

This collection of information is required by 37 CFR 1.31, 1.32 and 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: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

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

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

STATEMENT UNDER 37 CFR 3.73(b)

Applicant/Patent Owner: STEFIK, et al.

Application No./Patent No.: 13/585,408

Filed/Issue Date: August 14, 2012

Titled: SYSTEM AND METHOD FOR DISTRIBUTING DIGITAL CONTENT TO BE RENDERED IN ACCORDANCE WITH USAGE RIGHTS INFORMATION

ContentGuard Holdings, 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 in;
2. ☐ an assignee of less than the entire right, title, and interest in
(The extent (by percentage) of its ownership interest is _____ %); or
3. ☐ the assignee of an undivided interest in the entirety of (a complete assignment from one of the joint inventors was made)

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 therefore is attached.

OR

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

1. From: STEFIK, et al. To: Xerox Corporation

The document was recorded in the United States Patent and Trademark Office at
Reel 028922, Frame 0010, or for which a copy thereof is attached.

2. From: Xerox Corporation To: ContentGuard Holdings, Inc.

The document was recorded in the United States Patent and Trademark Office at
Reel 028922, Frame 0012, or for which a copy thereof is attached.

3. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at
Reel _____, Frame _____, or for which a copy thereof is attached.

☐ Additional documents in the chain of title are listed on a supplemental sheet(s).

- ☒ As required by 37 CFR 3.73(b)(1)(i), the documentary evidence of the chain of title from the original owner to the assignee was, or concurrently is being, submitted for recordation pursuant to 37 CFR 3.11.

[NOTE: A separate copy (i.e., a true copy of the original assignment document(s)) must be submitted to Assignment Division in accordance with 37 CFR Part 3, to record the assignment 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.

/Stephen M. Hertzler, Reg.No. 58,247/

Signature

September 17, 2012

Date

Stephen M. Hertzler

Printed or Typed Name

Attorney of Record

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.**

Privacy Act Statement

The **Privacy Act of 1974 (P.L. 93-579)** requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (*i.e.*, GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Electronic Acknowledgement Receipt

EFS ID:	13761824
Application Number:	13585408
International Application Number:	
Confirmation Number:	4941
Title of Invention:	SYSTEM AND METHOD FOR DISTRIBUTING DIGITAL CONTENT TO BE RENDERED IN ACCORDANCE WITH USAGE RIGHTS INFORMATION
First Named Inventor/Applicant Name:	Mark J. Stefik
Customer Number:	98804
Filer:	Stephen M. Hertzler
Filer Authorized By:	
Attorney Docket Number:	10-510-US-C73
Receipt Date:	17-SEP-2012
Filing Date:	14-AUG-2012
Time Stamp:	16:54:19
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	Power of Attorney	ContentGuard_-_2012-09-17_-_POA2.pdf	70290 e1556c9f79b440c12e45890bcecc6efa2e462be0	no	1

Warnings:

Information:

2	Assignee showing of ownership per 37 CFR 3.73(b).	10-510-US-C73_-2012-09-17-_Statement37CFR373B.pdf	456341 1581e95ac72a47f567b89224adee5e10237f7b0f	no	2
Warnings:					
Information:					
Total Files Size (in bytes):			526631		
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. <u>New Applications Under 35 U.S.C. 111</u> 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. <u>National Stage of an International Application under 35 U.S.C. 371</u> 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. <u>New International Application Filed with the USPTO as a Receiving Office</u> 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.					

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		13585408
	Filing Date		2012-08-14
	First Named Inventor	Mark J. STEFIK	
	Art Unit	2431	
	Examiner Name		
	Attorney Docket Number	10-510-US-C73	

U.S.PATENTS						Remove
Examiner Initial*	Cite No	Patent Number	Kind Code ¹	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Patent citation information please click the Add button.

Add

U.S.PATENT APPLICATION PUBLICATIONS						Remove
Examiner Initial*	Cite No	Publication Number	Kind Code ¹	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Published Application citation information please click the Add button.

Add

FOREIGN PATENT DOCUMENTS							Remove	
Examiner Initial*	Cite No	Foreign Document Number ³	Country Code ²	Kind Code ⁴	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T ⁵
	1							☐

If you wish to add additional Foreign Patent Document citation information please click the Add button

Add

NON-PATENT LITERATURE DOCUMENTS		Remove
Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.

T⁵

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number		13585408
Filing Date		2012-08-14
First Named Inventor	Mark J. STEFIK	
Art Unit	2431	
Examiner Name		
Attorney Docket Number	10-510-US-C73	

1	Non-Final Office Action dated June 12, 2008 cited in Application No. 11/304,793.	☐
2	Final Office Action dated November 14, 2008 cited in Application No. 11/304,793.	☐
3	Non- Final Office Action dated May 27, 2009 cited in Application No. 11/304,793.	☐
4	Final Office Action dated January 22, 2010 cited in Application No. 11/304,793.	☐
5	Decision on Appeal dated June 13, 2012 cited in Application No. 11/304,793.	☐

If you wish to add additional non-patent literature document citation information please click the Add button **Add**

EXAMINER SIGNATURE

Examiner Signature		Date Considered	

***EXAMINER:** Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

¹ See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. ² Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). ³ For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. ⁴ Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. ⁵ Applicant is to place a check mark here if English language translation is attached.

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	13585408
Filing Date	2012-08-14
First Named Inventor	Mark J. STEFIK
Art Unit	2431
Examiner Name	
Attorney Docket Number	10-510-US-C73

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

☐ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

☐ See attached certification statement.

☐ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Stephen M. Hertzler, Reg. No. 58,247/	Date (YYYY-MM-DD)	2012-09-21
Name/Print	Stephen M. Hertzler	Registration Number	58,247

This collection of information is required by 37 CFR 1.97 and 1.98. 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 1.14. This collection is estimated to take 1 hour 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.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these records.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
11/304,793	12/16/2005	Mark J. Stefik	111325-028300	6083
22204	7590	06/12/2008		
NIXON PEABODY, LLP 401 9TH STREET, NW SUITE 900 WASHINGTON, DC 20004-2128			EXAMINER BADII, BEHRANG	
			ART UNIT 3694	PAPER NUMBER
			MAIL DATE 06/12/2008	DELIVERY MODE PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No. 11/304,793	Applicant(s) STEFIK ET AL.	
	Examiner BEHRANG BADII	Art Unit 3694	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 16 December 2005.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-41 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-41 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 16 December 2005 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)	4) ☐ Interview Summary (PTO-413)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)	Paper No(s)/Mail Date. _____
3) ☒ Information Disclosure Statement(s) (PTO/SB/08)	5) ☐ Notice of Informal Patent Application
Paper No(s)/Mail Date <u>12/16/05, 8/25/06 & 2/19/08</u> .	6) ☐ Other: _____

DETAILED ACTION

Claims 1-41 have been examined.

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

Whoever 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, subject to the conditions and requirements of this title.

As per claims 1-41, based on Supreme Court precedent (Diamond v. Diehr, 450 U.S. 175, 184 (1981); Parker v. Flook, 437 U.S. 584, 588 n.9 (1978); Gottschalk v. Benson, 409 U.S. 63, 70 (1972); Cochrane v. Deener, 94 U.S. 780, 787-88 (1876).) and recent Federal Circuit decisions, the Office's guidance is that a 101 process must (1) be tied to another statutory class (such as a particular apparatus) or (2) transform underlying subject matter (such as an article or materials) to a different state or thing. (The Supreme Court recognizes that this test is not necessarily fixed or permanent and may evolve with technological advances. Gottschalk v. Benson, 409 U.S. 63, 71 (1972)). If neither of these requirements is met by the claim, the method is not a patent eligible process under 101.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 1-41 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. As per claims 1 and 22, the phrases "means for

creating usage rights from a grammar", "said means for creating comprises means for selecting one or more symbols from a first set of predetermined symbols to define a valid sequence of symbols to indicate the manner use, said means for creating comprises means for selecting symbols from a second set of predetermined symbols to define a valid sequence of symbols to indicate the conditions" are unclear. How is this creation being carried out? It is unclear how the usage rights are specifically being carried out? Further, the phrase "wherein the usage rights also specify one or more conditions which must be satisfied before the manner of use is exercised" is unclear. What are the specific one or more conditions, and the specific manner of use?

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claims 1 - 41 are rejected under 35 U.S.C. 103(a) as being unpatentable over Pinard et al., USP 5,638,494, and further in view of Rhoads, USP 7,035,427.

As per claims 1 and 22, Pinard discloses a system/method for associating usage rights with digital content, said system comprising: means for creating usage rights from a grammar, said usage rights specifying a manner of use indicating one or more stated purposes for which the digital content is at least one of used and distributed by an authorized party; means for processing a usage transaction specifying the usage rights to determine if access to the digital content is granted; and means for storing said usage

rights in a distributed repository, wherein the usage rights also specify one or more conditions which must be satisfied before the manner of use is exercised, said means for creating comprises means for selecting one or more symbols from a first set of predetermined symbols to define a valid sequence of symbols to indicate the manner use, said means for creating comprises means for selecting symbols from a second set of predetermined symbols to define a valid sequence of symbols to indicate the conditions (col.4, 24-65; col.7, 30-67; claims 17 & 35). Pinard does not disclose means for associating the usage rights with the digital content. Rhoads discloses means for associating the usage rights with the digital content (claim 1). It would have been obvious to modify Pinard to include means for associating the usage rights with the digital content such as that taught by Rhoads in order for the usage rights to be catalogued therein and be easily accessible for use for the parts that the usage rights are associated with (claim 1).

As per claim 2 and 23 Pinard discloses wherein the manner of use specifies a manner by which an authorized user is able to render the digital content (col.4, 24-65; col.7, 30-67; claims 17 & 35).

As per claims 3 and 24, Pinard discloses wherein the manner of use specifies the manner by which an authorized party uses the digital content to create a new digital content (col.4, 24-65; col.7, 30-67; claims 17 & 35).

As per claims 4 and 25, Pinard discloses wherein the manner of use specifies the manner by which an authorized party is able to make a back-up copy of the digital content (col.4, 24-65; col.7, 30-67; claims 17 & 35).

As per claims 5 and 26, Pinard discloses wherein the manner of use specifies the manner by which an authorized party is able to conceal the corresponding digital content on a device on which the digital content is stored (col.4, 24-65; col.7, 30-67; claims 17 & 35).

As per claims 6 and 27, Pinard discloses wherein the manner of use specifies the manner by which an authorized party is able to delete the digital content from a device on which digital content is stored (col.4, 24-65; col.7, 30-67; claims 17 & 35).

As per claims 7 and 28, Pinard discloses wherein the digital content is a software program (col.4, 24-65; col.7, 30-67; claims 17 & 35).

As per claims 8 and 29, Pinard discloses wherein the manner of use specifies the manner by which an authorized party is able to install the software program (col.4, 24-65; col.7, 30-67; claims 17 & 35).

As per claims 9 and 30, Pinard discloses wherein the manner of use specifies the manner by which an authorized party is able to uninstall the software program (col.4, 24-65; col.7, 30-67; claims 17 & 35).

As per claims 10 and 31, Pinard discloses wherein the usage rights comprise a revenue identifier for identifying a revenue owner of the digital content (col.4, 24-65; col.7, 30-67; claims 17 & 35).

As per claims 11 and 32, Pinard discloses wherein the usage rights comprise a class identifier for identifying a class of rendering devices upon which the digital content is rendered (col.4, 24-65; col.7, 30-67; claims 17 & 35).

As per claims 12 and 33, Pinard discloses wherein said means for creating comprises means for creating a first version of usage rights having a first set of conditions and means for creating a second version of usage rights having a second set of conditions (col.4, 24-65; col.7, 30-67; claims 17 & 35).

As per claims 13 and 34, Pinard discloses wherein said means for creating comprises means for selecting one or more codes from a set of predetermined codes to define a valid sequence of codes to indicate the manner of use (col.4, 24-65; col.7, 30-67; claims 17 & 35).

As per claims 14 and 35, Pinard discloses wherein said means for creating comprises means for selecting one or more identifiers from a set of predetermined identifiers to define a valid sequence of identifiers to indicate the manner of use (col.4, 24-65; col.7, 30-67; claims 17 & 35).

As per claims 15 and 36, Pinard discloses wherein said means for creating comprises means for selecting one or more parameters from a set of predetermined parameters to define a valid sequence of parameters to indicate the manner of use (col.4, 24-65; col.7, 30-67; claims 17 & 35).

As per claim 16, Pinard discloses wherein said means for creating and said means for designating, and said means for associating each comprise computer readable instructions recorded on media (col.4, 24-65; col.7, 30-67; claims 17 & 35).

As per claims 17 and 37, Pinard discloses wherein said means for creating comprises means for designating a set of default conditions, and means for changing the default set of conditions (col.4, 24-65; col.7, 30-67; claims 17 & 35).

As per claims 18 and 38, Pinard discloses wherein said usage rights are stored on removable storage media (col.4, 24-65; col.7, 30-67; claims 17 & 35).

As per claim 19, Pinard discloses wherein said system is implemented via one or more hardware and software devices (col.4, 24-65; col.7, 30-67; claims 17 & 35).

As per claims 20 and 40, Pinard discloses wherein the usage rights and the digital content are stored in the distributed repository (col.4, 24-65; col.7, 30-67; claims 17 & 35).

As per claims 21 and 41, Pinard discloses wherein the digital content is stored in a repository that is different from the distributed repository (col.4, 24-65; col.7, 30-67; claims 17 & 35).

As per claim 39, Pinard discloses wherein the method is implemented via one or more computer readable instructions recorded on a computer readable medium and configured to cause one or more computer processors to perform the steps of said method (col.4, 24-65; col.7, 30-67; claims 17 & 35).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Behrang Badii whose telephone number is 571-272-6879. The examiner can normally be reached on Monday-Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, James Trammell can be reached on 571-272-6712. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Any response to this action should be mailed to:

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

or faxed to (571)273-8300

Hand delivered responses should be brought to

United States Patent and Trademark Office
Customer Service Window
Randolph Building
401 Dulany Street
Alexandria, VA 22314

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the Technology Center 3600 Customer Service Office whose telephone number is **(571) 272-3600**.

/BB/

/James P Trammell/

Application/Control Number: 11/304,793

Page 9

Art Unit: 3694

Supervisory Patent Examiner, Art Unit 3694



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
11/304,793	12/16/2005	Mark J. Stefik	111325-028300	6083
22204	7590	11/14/2008	EXAMINER	
NIXON PEABODY, LLP 401 9TH STREET, NW SUITE 900 WASHINGTON, DC 20004-2128			BADII, BEHRANG	
			ART UNIT	PAPER NUMBER
			3694	
			MAIL DATE	DELIVERY MODE
			11/14/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No. 11/304,793	Applicant(s) STEFIK ET AL.	
	Examiner BEHRANG BADII	Art Unit 3694	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 21 July 2008.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 42-59 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 42-59 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)	4) ☐ Interview Summary (PTO-413)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)	Paper No(s)/Mail Date. _____
3) ☒ Information Disclosure Statement(s) (PTO/SB/08)	5) ☐ Notice of Informal Patent Application
Paper No(s)/Mail Date <u>6/17/08, 10/09/08</u> .	6) ☐ Other: _____

DETAILED ACTION

Response to Arguments

Applicant's arguments with respect to claims 42-59 have been considered but are moot in view of the new ground(s) of rejection.

Claims 1-41 are cancelled.

Claims 24-59 have been examined.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 42-59 are rejected under 35 U.S.C. 102(e) as being disclosed by Wyman, USP 5,438,508.

As per claim 42, 48 and 54, Wyman discloses a method/system/repository of rendering digital content in accordance with usage rights information, the usage rights information specifying a manner by which the digital content may be rendered, the method comprising: establishing trust for receiving the digital content; receiving the digital content (abstract; col.6, 48-68; col.13, 14-68; col.14, 1-16; fig's 5&6) ; receiving a request to render the digital content (abstract; col.6, 48-68; col.13, 14-68; col.14, 1-16; fig's 5&6); determining, based on the usage rights information, whether the content may

Art Unit: 3694

be rendered in accordance with the request (abstract; col.6, 48-68; col.13, 14-68; col.14, 1-16; fig's 5&6); rendering the digital content in accordance with the request only if it is determined that the content may be rendered in accordance with the request (abstract; col.6, 48-68; col.13, 14-68; col.14, 1-16; fig's 5&6); and denying the request and preventing rendering of the digital content if it is determined that the digital content may not be rendered in accordance with the request (abstract; col.6, 48-68; col.13, 14-68; col.14, 1-16; fig's 5&6).

As per claim 43, 49 and 55, Wyman further discloses wherein the usage rights information further includes a condition under which the manner of use can be granted, and the determining step further includes determining whether the condition is satisfied (abstract; col.6, 48-68; col.13, 14-68; col.14, 1-16; fig's 5&6).

As per claim 44, 50 and 56, Wyman further discloses making a request for an authorization object required to render the digital content; and receiving the authorization object when it is determined that the request should be granted (abstract; col.6, 48-68; col.13, 14-68; col.14, 1-16; fig's 5&6).

As per claim 45, 51 and 57, Wyman further discloses making a request for an authorization object required to be included within a repository for the repository to make the digital work available for use, the authorization object being further required to receive the digital work and during use of the digital work; determining whether the request for an authorization object from the repository should be granted; and transmitting the authorization object to the repository if the request for the authorization

Art Unit: 3694

object from the repository should be granted (abstract; col.6, 48-68; col.13, 14-68; col.14, 1-16; fig's 5&6).

As per claim 46, 52 and 58 Wyman further discloses generating a registration message at a recipient repository, the registration message including an identification certificate of the recipient repository and a random registration identifier, the identification certificate being certified by a master repository; receiving the registration message at a provider repository; validating at the provider repository the authenticity of the recipient repository; exchanging messages including at least one session key between the provider and recipient repositories, the session key to be used in communications during a session between the provider and recipient repositories; and conducting a secure transaction between the provider and recipient repositories using the session key, wherein the secure transaction includes sending the digital work to the recipient repository (abstract; col.6, 48-68; col.13, 14-68; col.14, 1-16; fig's 5&6).

As per claim 47, 53 and 59 Wyman further discloses verifying the identification certificate of the recipient repository; generating at the provider repository a message to test the authenticity of the recipient repository, the generated message including a nonce; sending the generated message to the recipient repository; and verifying at the provider repository if the recipient repository correctly processed the generated message (abstract; col.6, 48-68; col.13, 14-68; col.14, 1-16; fig's 5&6).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

Art Unit: 3694

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claims 42-59 are rejected under 35 U.S.C. 103(a) as being unpatentable over Wyman, USP 5,438,508, and further in view of Pinard et al., USP 5,638,494.

As per claim 42, 48 and 54, Wyman discloses a method/system/repository of rendering digital content in accordance with usage rights information, the usage rights information specifying a manner by which the digital content may be rendered, the method comprising: establishing trust for receiving the digital content; receiving the digital content (abstract; col.6, 48-68; col.13, 14-68; col.14, 1-16; fig's 5&6) ; receiving a request to render the digital content (abstract; col.6, 48-68; col.13, 14-68; col.14, 1-16; fig's 5&6); rendering the digital content in accordance with the request only if it is determined that the content may be rendered in accordance with the request (abstract; col.6, 48-68; col.13, 14-68; col.14, 1-16; fig's 5&6); and denying the request and preventing rendering of the digital content if it is determined that the digital content may not be rendered in accordance with the request (abstract; col.6, 48-68; col.13, 14-68; col.14, 1-16; fig's 5&6). Wyman might not disclose determining, based on the usage rights information, whether the content may be rendered in accordance with the request. Pinard discloses determining, based on the usage rights information, whether the content may be rendered in accordance with the request (col.6, 41-68; col.7, 14-22; fig 3c). It would have been obvious to modify Wyman to include determining, based on the usage rights information, whether the content may be rendered in accordance with the request such as that taught by Pinard in order to so that the system can be used to

Art Unit: 3694

manage the flow of work, detect and correct inefficiencies, negotiate service with outside systems, and can be tightly integrated with and adapt to the human based user organization's work processes and goals (Pinard, col.1, 42-45).

As per claim 43, 49 and 55, Wyman further discloses wherein the usage rights information further includes a condition under which the manner of use can be granted, and the determining step further includes determining whether the condition is satisfied (abstract; col.6, 48-68; col.13, 14-68; col.14, 1-16; fig's 5&6).

As per claim 44, 50 and 56, Wyman further discloses making a request for an authorization object required to render the digital content; and receiving the authorization object when it is determined that the request should be granted (abstract; col.6, 48-68; col.13, 14-68; col.14, 1-16; fig's 5&6).

As per claim 45, 51 and 57, Wyman further discloses making a request for an authorization object required to be included within a repository for the repository to make the digital work available for use, the authorization object being further required to receive the digital work and during use of the digital work; determining whether the request for an authorization object from the repository should be granted; and transmitting the authorization object to the repository if the request for the authorization object from the repository should be granted (abstract; col.6, 48-68; col.13, 14-68; col.14, 1-16; fig's 5&6).

As per claim 46, 52 and 58 Wyman further discloses generating a registration message at a recipient repository, the registration message including an identification certificate of the recipient repository and a random registration identifier, the

Art Unit: 3694

identification certificate being certified by a master repository; receiving the registration message at a provider repository; validating at the provider repository the authenticity of the recipient repository; exchanging messages including at least one session key between the provider and recipient repositories, the session key to be used in communications during a session between the provider and recipient repositories; and conducting a secure transaction between the provider and recipient repositories using the session key, wherein the secure transaction includes sending the digital work to the recipient repository (abstract; col.6, 48-68; col.13, 14-68; col.14, 1-16; fig's 5&6).

As per claim 47, 53 and 59 Wyman further discloses verifying the identification certificate of the recipient repository; generating at the provider repository a message to test the authenticity of the recipient repository, the generated message including a nonce; sending the generated message to the recipient repository; and verifying at the provider repository if the recipient repository correctly processed the generated message (abstract; col.6, 48-68; col.13, 14-68; col.14, 1-16; fig's 5&6).

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 42-59 rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. It is unclear as to how “establishing trust for receiving the digital content” is carried out.

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

Whoever 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, subject to the conditions and requirements of this title.

Claims 42-59 are rejected under 35 U.S.C. 101 because based on Supreme Court precedent (*Diamond v. Diehr*, 450 U.S. 175, 184 (1981); *Parker v. Flook*, 437 U.S. 584, 588 n.9 (1978); *Gottschalk v. Benson*, 409 U.S. 63, 70 (1972); *Cochrane v. Deener*, 94 U.S. 780, 787-88 (1876).) and recent Federal Circuit decisions, the Office's guidance is that a 101 process must (1) be tied to another statutory class (such as a particular apparatus) or (2) transform underlying subject matter (such as an article or materials) to a different state or thing. (The Supreme Court recognizes that this test is not necessarily fixed or permanent and may evolve with technological advances. *Gottschalk v. Benson*, 409 U.S. 63, 71 (1972)). If neither of these requirements is met by the claim, the method is not a patent eligible process under 101.

Double Patenting

The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. A nonstatutory obviousness-type double patenting rejection is appropriate where the conflicting claims are not identical, but at least one examined application claim is not patentably distinct from the reference claim(s) because the examined application claim is either anticipated by, or would have been obvious over, the reference claim(s). See, e.g., *In re Berg*, 140 F.3d 1428, 46 USPQ2d 1226 (Fed. Cir. 1998); *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); and *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) or 1.321(d) may be used to overcome an actual or provisional rejection based on a nonstatutory

Art Unit: 3694

double patenting ground provided the conflicting application or patent either is shown to be commonly owned with this application, or claims an invention made as a result of activities undertaken within the scope of a joint research agreement.

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

Claims 42-59 rejected on the ground of nonstatutory double patenting over claims 1-23 of U. S. Patent No. 6,708,157 and claims 1-45 of USP 7,266,529 since the claims, if allowed, would improperly extend the "right to exclude" already granted in the patent.

The subject matter claimed in the instant application is fully disclosed in the patent and is covered by the patent since the patent and the application are claiming common subject matter, as follows: Rendering digital content in accordance with usage rights information, the usage rights information specifying a manner by which the digital content may be rendered.

Furthermore, there is no apparent reason why applicant was prevented from presenting claims corresponding to those of the instant application during prosecution of the application which matured into a patent. See *In re Schneller*, 397 F.2d 350, 158 USPQ 210 (CCPA 1968). See also MPEP § 804.

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within

Art Unit: 3694

TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Behrang Badii whose telephone number is 571-272-6879. The examiner can normally be reached on Monday-Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, James Trammell can be reached on 571-272-6712. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Any response to this action should be mailed to:

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

or faxed to (571)273-8300

Hand delivered responses should be brought to

United States Patent and Trademark Office
Customer Service Window
Randolph Building
401 Dulany Street
Alexandria, VA 22314

Any inquiry of a general nature or relating to the status of this application
or proceeding should be directed to the Technology Center 3600 Customer Service
Office whose telephone number is **(571) 272-3600**.

/BB/

/James P Trammell/
Supervisory Patent Examiner, Art Unit 3694



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
11/304,793	12/16/2005	Mark J. Stefik	111325-028300	6083
22204	7590	05/27/2009	EXAMINER	
NIXON PEABODY, LLP 401 9TH STREET, NW SUITE 900 WASHINGTON, DC 20004-2128			BADII, BEHRANG	
			ART UNIT	PAPER NUMBER
			3694	
			MAIL DATE	DELIVERY MODE
			05/27/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No. 11/304,793	Applicant(s) STEFIK ET AL.	
	Examiner BEHRANG BADII	Art Unit 3694	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 11 February 2009.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 42-59 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 42-59 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)	4) ☐ Interview Summary (PTO-413)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)	Paper No(s)/Mail Date. _____
3) ☒ Information Disclosure Statement(s) (PTO/SB/08)	5) ☐ Notice of Informal Patent Application
Paper No(s)/Mail Date <u>12/31/08</u> .	6) ☐ Other: _____

DETAILED ACTION

Response to Arguments

Applicant's arguments filed on 2/11/09 have been fully considered but they are not persuasive. As per the 101 rejection, the 101 rejection for claims 48-52 has been withdrawn. Although there have been changes to the preamble of the independent claims, it is the changes to the actual claim limitations (the body of the claims) that would overcome a 101 rejection. The 101 rejection for claims 42-47 and 54-59 is not withdrawn due to insufficient changes to the claims' limitations to overcome this rejection. The 112 2nd paragraph rejection is discussed below. Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

The double patenting is given until a terminal disclaimer is filed. As per the art rejection, the applicant's main argument is that the prior art does not disclose the limitations "establishing trust for receiving the digital content" and "determining, based on the usage rights information, whether the content may be rendered in accordance with the request, wherein the usage rights information specifies a manner by which the digital content may be rendered". These two limitations are not clear as discussed in the 112 rejection below. In response to applicant's argument that the above are not disclosed, a recitation of the intended use of the claimed invention must result in a structural difference between the claimed invention and the prior art in order to patentably distinguish the claimed invention from the prior art. If the prior art structure is capable of performing the intended use, then it meets the claim.

Further, “establishing trust for receiving the digital content” is disclosed by Wyman by being in contact with the receiver and examining is the request is permitted. Establishing trust is also inherent in the prior art. Also, Pinard discloses “determining, based on the usage rights information, whether the content may be rendered in accordance with the request, wherein the usage rights information specifies a manner by which the digital content may be rendered” as discussed below.

2112 [R-3] Requirements of Rejection Based on Inherency; Burden of Proof

The express, implicit, and inherent disclosures of a prior art reference may be relied upon in the rejection of claims under 35 U.S.C. 102 or 103. “The inherent teaching of a prior art reference, a question of fact, arises both in the context of anticipation and obviousness.” In re Napier, 55 F.3d 610, 613, 34 USPQ2d 1782, 1784 (Fed. Cir. 1995) (affirmed a 35 U.S.C. 103 rejection based in part on inherent disclosure in one of the references). See also In re Grasselli, 713 F.2d 731, 739, 218 USPQ 769, 775 (Fed. Cir. 1983).

Claims 1-41 are cancelled.

Claims 42-59 have been examined.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 42-59 rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. It is unclear as to how “establishing trust for

Art Unit: 3694

receiving the digital content” is carried out. Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

Further, the limitation “determining, based on the usage rights information, whether the content may be rendered in accordance with the request, wherein the usage rights information specifies a manner by which the digital content may be rendered” is unclear. How does, the manner by which the digital content may be rendered, has anything to do with the determination of whether or not the content may be rendered?

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

Whoever 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, subject to the conditions and requirements of this title.

Claims 42-47 are rejected under 35 U.S.C. 101 because based on Supreme Court precedent (*Diamond v. Diehr*, 450 U.S. 175, 184 (1981); *Parker v. Flook*, 437 U.S. 584, 588 n.9 (1978); *Gottschalk v. Benson*, 409 U.S. 63, 70 (1972); *Cochrane v. Deener*, 94 U.S. 780, 787-88 (1876).) and recent Federal Circuit decisions, the Office’s guidance is that a 101 process must (1) be tied to another statutory class (such as a particular apparatus) or (2) transform underlying subject matter (such as an article or materials) to a different state or thing. (The Supreme Court recognizes that this test is not necessarily fixed or permanent and may evolve with technological advances. *Gottschalk v. Benson*, 409 U.S. 63, 71 (1972)). If neither of these requirements is met by the claim, the method is not a patent eligible process under 101.

Claims 54-59 are rejected under 35 U.S.C. 101 because the claims are directed to a repository for rendering digital content. The rendering of digital content is deemed to be descriptive data that cannot exhibit any functional interrelationship with the way in which computing processes are performed and does not constitute a statutory process, machine, manufacture or composition of matter. When non-functional descriptive data is rendered on some computer-readable medium, it is not structurally and functionally interrelated to the medium but is merely carried by the medium. Thus, claims 54-59 are deemed to be non-statutory.

Double Patenting

The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the “right to exclude” granted by a patent and to prevent possible harassment by multiple assignees. A nonstatutory obviousness-type double patenting rejection is appropriate where the conflicting claims are not identical, but at least one examined application claim is not patentably distinct from the reference claim(s) because the examined application claim is either anticipated by, or would have been obvious over, the reference claim(s). See, e.g., *In re Berg*, 140 F.3d 1428, 46 USPQ2d 1226 (Fed. Cir. 1998); *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); and *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) or 1.321(d) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent either is shown to be commonly owned with this application, or claims an invention made as a result of activities undertaken within the scope of a joint research agreement.

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

Claims 42-59 rejected on the ground of nonstatutory double patenting over claims 1-23 of U. S. Patent No. 6,708,157 and claims 1-45 of USP 7,266,529 since the claims, if allowed, would improperly extend the "right to exclude" already granted in the patent.

The subject matter claimed in the instant application is fully disclosed in the patent and is covered by the patent since the patent and the application are claiming common subject matter, as follows: Rendering digital content in accordance with usage rights information, the usage rights information specifying a manner by which the digital content may be rendered.

Furthermore, there is no apparent reason why applicant was prevented from presenting claims corresponding to those of the instant application during prosecution of the application which matured into a patent. See *In re Schneller*, 397 F.2d 350, 158 USPQ 210 (CCPA 1968). See also MPEP § 804.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

At the outset, non-function descriptive materials are not given patentable weight. The prior art has been referenced to disclose all of these non-functional descriptive material even though non-functional descriptive materials are not given patentable weight.

Claims 42-59 are rejected under 35 U.S.C. 102(e) as being disclosed by Wyman, USP 5,438,508.

As per claim 42, 48 and 54, Wyman discloses a method/system/repository of rendering digital content in accordance with usage rights information, the usage rights information specifying a manner by which the digital content may be rendered, the method comprising: establishing trust for receiving the digital content (nonfunctional descriptive); receiving the digital content at the recipient repository (database) (nonfunctional descriptive) (abstract; col.6, 48-68; col.13, 14-68; col.14, 1-16; fig's 5&6) ; receiving a request at the recipient repository to render the digital content (nonfunctional descriptive) (abstract; col.6, 48-68; col.13, 14-68; col.14, 1-16; fig's 5&6); determining, based on the usage rights information, whether the content may be rendered in accordance with the request, wherein the usage rights information specifies a manner by which the digital content may be rendered (abstract; col.6, 48-68; col.13, 14-68; col.14, 1-16; fig's 5&6); rendering the digital content in accordance with the request only if it is determined that the content may be rendered in accordance with the request (abstract; col.6, 48-68; col.13, 14-68; col.14, 1-16; fig's 5&6); and denying the request and preventing rendering of the digital content if it is determined that the digital

content may not be rendered in accordance with the request (abstract; col.6, 48-68; col.13, 14-68; col.14, 1-16; fig's 5&6).

As per claim 43, 49 and 55, Wyman further discloses wherein the usage rights information further includes a condition under which the manner of use can be granted, and the determining step further includes determining whether the condition is satisfied (abstract; col.6, 48-68; col.13, 14-68; col.14, 1-16; fig's 5&6).

As per claim 44, 50 and 56, Wyman further discloses making a request from the recipient repository for an authorization object required to render the digital content; and receiving the authorization object at the recipient repository when it is determined that the request should be granted (abstract; col.6, 48-68; col.13, 14-68; col.14, 1-16; fig's 5&6).

As per claim 45, 51 and 57, Wyman further discloses making a request from the recipient repository for an authorization object for the recipient repository to make the digital content available for use, the authorization object being further required to receive the digital content and to use the digital content; determining whether the request from the recipient repository for the authorization object should be granted; and transmitting the authorization object to the recipient repository if it is determined that the request for the authorization object should be granted (abstract; col.6, 48-68; col.13, 14-68; col.14, 1-16; fig's 5&6).

As per claim 46, 52 and 58 Wyman further discloses generating a registration message at the recipient repository, the registration message including an identification certificate of the recipient repository and a random registration identifier, the

Art Unit: 3694

identification certificate being certified by a master repository; receiving the registration message at a provider repository; validating at the provider repository the authenticity of the recipient repository; exchanging messages including at least one session key between the provider repository and the recipient repository, the session key to be used in communications during a session between the provider repository and the recipient repository; and conducting a secure transaction between the provider repository and the recipient repository using the session key, wherein the secure transaction includes sending the digital content to the recipient repository (abstract; col.6, 48-68; col.13, 14-68; col.14, 1-16; fig's 5&6).

As per claim 47, 53 and 59 Wyman further discloses verifying the identification certificate of the recipient repository; generating at the provider repository a message to test the authenticity of the recipient repository, the generated message including a nonce; sending the generated message to the recipient repository; and verifying at the provider repository if the recipient repository correctly processed the generated message (abstract; col.6, 48-68; col.13, 14-68; col.14, 1-16; fig's 5&6).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

At the outset, non-function descriptive materials are not given patentable weight.

The prior art has been referenced to disclose all of these non-functional descriptive

Art Unit: 3694

material even though non-functional descriptive materials are not given patentable weight.

Claims 42-59 are rejected under 35 U.S.C. 103(a) as being unpatentable over Wyman, USP 5,438,508, and further in view of Pinard et al., USP 5,638,494.

As per claim 42, 48 and 54, Wyman discloses a method/system/repository of rendering digital content in accordance with usage rights information, the usage rights information specifying a manner by which the digital content may be rendered, the method comprising: establishing trust for receiving the digital content (nonfunctional descriptive); receiving the digital content at the recipient repository (nonfunctional descriptive) (abstract; col.6, 48-68; col.13, 14-68; col.14, 1-16; fig's 5&6) ; receiving a request at the recipient repository to render the digital content (nonfunctional descriptive) (abstract; col.6, 48-68; col.13, 14-68; col.14, 1-16; fig's 5&6); rendering the digital content in accordance with the request only if it is determined that the content may be rendered in accordance with the request (abstract; col.6, 48-68; col.13, 14-68; col.14, 1-16; fig's 5&6); and denying the request and preventing rendering of the digital content if it is determined that the digital content may not be rendered in accordance with the request (abstract; col.6, 48-68; col.13, 14-68; col.14, 1-16; fig's 5&6). Wyman might not disclose determining, based on the usage rights information, whether the content may be rendered in accordance with the request, wherein the usage rights information specifies a manner by which the digital content may be rendered. Pinard discloses determining, based on the usage rights information, whether the content may be rendered in accordance with the request, wherein the usage rights information

Art Unit: 3694

specifies a manner by which the digital content may be rendered (col.6, 41-68; col.7, 14-22; fig 3c). It would have been obvious to modify Wyman to include determining, based on the usage rights information, whether the content may be rendered in accordance with the request, wherein the usage rights information specifies a manner by which the digital content may be rendered such as that taught by Pinard in order to so that the system can be used to manage the flow of work, detect and correct inefficiencies, negotiate service with outside systems, and can be tightly integrated with and adapt to the human based user organization's work processes and goals (Pinard, col.1, 42-45).

As per claim 43, 49 and 55, Wyman further discloses wherein the usage rights information further includes a condition under which the manner of use can be granted, and the determining step further includes determining whether the condition is satisfied (abstract; col.6, 48-68; col.13, 14-68; col.14, 1-16; fig's 5&6).

As per claim 44, 50 and 56, Wyman further discloses making a request from the recipient repository for an authorization object required to render the digital content; and receiving the authorization object at the recipient repository when it is determined that the request should be granted (abstract; col.6, 48-68; col.13, 14-68; col.14, 1-16; fig's 5&6).

As per claim 45, 51 and 57, Wyman further discloses making a request from the recipient repository for an authorization object for the recipient repository to make the digital content available for use, the authorization object being further required to receive the digital content and to use the digital content; determining whether the

Art Unit: 3694

request from the recipient repository for the authorization object should be granted; and transmitting the authorization object to the recipient repository if it is determined that the request for the authorization object should be granted (abstract; col.6, 48-68; col.13, 14-68; col.14, 1-16; fig's 5&6).

As per claim 46, 52 and 58 Wyman further discloses generating a registration message at the recipient repository, the registration message including an identification certificate of the recipient repository and a random registration identifier, the identification certificate being certified by a master repository; receiving the registration message at a provider repository; validating at the provider repository the authenticity of the recipient repository; exchanging messages including at least one session key between the provider repository and the recipient repository, the session key to be used in communications during a session between the provider repository and the recipient repository; and conducting a secure transaction between the provider repository and the recipient repository using the session key, wherein the secure transaction includes sending the digital content to the recipient repository (abstract; col.6, 48-68; col.13, 14-68; col.14, 1-16; fig's 5&6).

As per claim 47, 53 and 59 Wyman further discloses verifying the identification certificate of the recipient repository; generating at the provider repository a message to test the authenticity of the recipient repository, the generated message including a nonce; sending the generated message to the recipient repository; and verifying at the provider repository if the recipient repository correctly processed the generated message (abstract; col.6, 48-68; col.13, 14-68; col.14, 1-16; fig's 5&6).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Behrang Badii whose telephone number is 571-272-6879. The examiner can normally be reached on Monday-Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, James Trammell can be reached on 571-272-6712. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Any response to this action should be mailed to:

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

or faxed to (571)273-8300

Hand delivered responses should be brought to

United States Patent and Trademark Office
Customer Service Window

Art Unit: 3694

Randolph Building
401 Dulany Street
Alexandria, VA 22314

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the Technology Center 3600 Customer Service Office whose telephone number is **(571) 272-3600**.

/Behrang Badii/
Examiner, Art Unit 3694



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
11/304,793	12/16/2005	Mark J. Stefik	111325-028300	6083
22204	7590	01/22/2010		
NIXON PEABODY, LLP 401 9TH STREET, NW SUITE 900 WASHINGTON, DC 20004-2128			EXAMINER BADII, BEHRANG	
			ART UNIT 3694	PAPER NUMBER
			MAIL DATE 01/22/2010	DELIVERY MODE PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No. 11/304,793	Applicant(s) STEFIK ET AL.	
	Examiner BEHRANG BADII	Art Unit 3694	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 01 October 2009.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 42-59 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 42-59 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)	4) ☐ Interview Summary (PTO-413)
2) ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)	Paper No(s)/Mail Date. _____
3) ☐ Information Disclosure Statement(s) (PTO/SB/08)	5) ☐ Notice of Informal Patent Application
Paper No(s)/Mail Date _____	6) ☐ Other: _____

DETAILED ACTION

Response to Arguments

Applicant's arguments filed on 10/1/09 have been fully considered but they are not persuasive. Applicant's arguments clarify the manner of how trust is established by noting "that very specific mechanisms for establishing trust are recited in claims 44 and 45". Hence, trust is established by authorization mechanisms. Authorization mechanisms are disclosed by the prior art as discussed below. Further, applicant concedes that Wyman established trust. However, applicant argues that the trust established by Wyman is not for the purpose of receiving the digital content. Wyman discloses that trust (authorization) is disclosed and this trust is disclosed for many reasons, one of which is for the purpose of receiving the digital content as discussed below (abstract; col.6, 48-68; col.13, 14-68; col.14, 1-16; fig's 5&6).

The double patenting is given until a terminal disclaimer is filed.

Further, "establishing trust for receiving the digital content" is disclosed by Wyman by being in contact with the receiver and examining is the request is permitted. Establishing trust is also inherent in the prior art. Also, Pinard discloses "determining, based on the usage rights information indicating a manner of use by which the digital content may be rendered, whether the content may be rendered in accordance with a specified manner" as discussed below.

A recitation of the intended use of the claimed invention must result in a structural difference between the claimed invention and the prior art in order to

Art Unit: 3694

patentably distinguish the claimed invention from the prior art. If the prior art structure is capable of performing the intended use, then it meets the claim.

2112 [R-3] Requirements of Rejection Based on Inherency; Burden of Proof

The express, implicit, and inherent disclosures of a prior art reference may be relied upon in the rejection of claims under 35 U.S.C. 102 or 103. "The inherent teaching of a prior art reference, a question of fact, arises both in the context of anticipation and obviousness." In re Napier, 55 F.3d 610, 613, 34 USPQ2d 1782, 1784 (Fed. Cir. 1995) (affirmed a 35 U.S.C. 103 rejection based in part on inherent disclosure in one of the references). See also In re Grasselli, 713 F.2d 731, 739, 218 USPQ 769, 775 (Fed. Cir. 1983).

Claims 1-41 are cancelled.

Claims 42-59 have been examined.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

At the outset, non-function descriptive materials are not given patentable weight. The prior art has been referenced to disclose all of these non-functional descriptive material even though non-functional descriptive materials are not given patentable weight.

Claims 42-59 are rejected under 35 U.S.C. 103(a) as being unpatentable over Wyman, USP 5,438,508, and further in view of Pinard et al., USP 5,638,494.

As per claim 42, 48 and 54, Wyman discloses a method/system/repository of rendering digital content in accordance with usage rights information, the usage rights information specifying a manner by which the digital content may be rendered, the method comprising: establishing trust for the purpose of receiving the digital content (nonfunctional descriptive) (abstract; col.6, 48-68; col.13, 14-68; col.14, 1-16; fig's 5&6); after said establishing step, receiving the digital content at the recipient repository (nonfunctional descriptive) (abstract; col.6, 48-68; col.13, 14-68; col.14, 1-16; fig's 5&6); receiving a request at the recipient repository to render the digital content (nonfunctional descriptive) (abstract; col.6, 48-68; col.13, 14-68; col.14, 1-16; fig's 5&6); rendering the digital content in accordance with the specified manner only if it is determined that the content may be rendered in accordance with the specified manner (abstract; col.6, 48-68; col.13, 14-68; col.14, 1-16; fig's 5&6); and denying the request and preventing rendering of the digital content if it is determined that the digital content may not be rendered in accordance with the specified manner (abstract; col.6, 48-68; col.13, 14-68; col.14, 1-16; fig's 5&6). Wyman might not disclose determining, based on the usage rights information indicating a manner of use by which the digital content may be rendered, whether the content may be rendered in accordance with a specified manner. Pinard discloses determining, based on the usage rights information indicating a manner of use by which the digital content may be rendered, whether the content may be rendered in accordance with a specified manner (col.6, 41-68; col.7, 14-22; fig 3c). It

Art Unit: 3694

would have been obvious to modify Wyman to include determining, based on the usage rights information indicating a manner of use by which the digital content may be rendered, whether the content may be rendered in accordance with a specified manner, such as that taught by Pinard in order to so that the system can be used to manage the flow of work, detect and correct inefficiencies, negotiate service with outside systems, and can be tightly integrated with and adapt to the human based user organization's work processes and goals (Pinard, col.1, 42-45).

As per claim 43, 49 and 55, Wyman further discloses wherein the usage rights information further includes a condition under which the manner of use can be granted, and the determining step further includes determining whether the condition is satisfied (abstract; col.6, 48-68; col.13, 14-68; col.14, 1-16; fig's 5&6).

As per claim 44, 50 and 56, Wyman further discloses making a request from the recipient repository for an authorization object required to render the digital content; and receiving the authorization object at the recipient repository when it is determined that the request should be granted (abstract; col.6, 48-68; col.13, 14-68; col.14, 1-16; fig's 5&6).

As per claim 45, 51 and 57, Wyman further discloses making a request from the recipient repository for an authorization object for the recipient repository to make the digital content available for use, the authorization object being further required to receive the digital content and to use the digital content; determining whether the request from the recipient repository for the authorization object should be granted; and transmitting the authorization object to the recipient repository if it is determined that the

Art Unit: 3694

request for the authorization object should be granted (abstract; col.6, 48-68; col.13, 14-68; col.14, 1-16; fig's 5&6).

As per claim 46, 52 and 58 Wyman further discloses generating a registration message at the recipient repository, the registration message including an identification certificate of the recipient repository and a random registration identifier, the identification certificate being certified by a master repository; receiving the registration message at a provider repository; validating at the provider repository the authenticity of the recipient repository; exchanging messages including at least one session key between the provider repository and the recipient repository, the session key to be used in communications during a session between the provider repository and the recipient repository; and conducting a secure transaction between the provider repository and the recipient repository using the session key, wherein the secure transaction includes sending the digital content to the recipient repository (abstract; col.6, 48-68; col.13, 14-68; col.14, 1-16; fig's 5&6).

As per claim 47, 53 and 59 Wyman further discloses verifying the identification certificate of the recipient repository; generating at the provider repository a message to test the authenticity of the recipient repository, the generated message including a nonce; sending the generated message to the recipient repository; and verifying at the provider repository if the recipient repository correctly processed the generated message (abstract; col.6, 48-68; col.13, 14-68; col.14, 1-16; fig's 5&6).

Double Patenting

The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the

Art Unit: 3694

unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. A nonstatutory obviousness-type double patenting rejection is appropriate where the conflicting claims are not identical, but at least one examined application claim is not patentably distinct from the reference claim(s) because the examined application claim is either anticipated by, or would have been obvious over, the reference claim(s). See, e.g., *In re Berg*, 140 F.3d 1428, 46 USPQ2d 1226 (Fed. Cir. 1998); *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); and *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) or 1.321(d) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent either is shown to be commonly owned with this application, or claims an invention made as a result of activities undertaken within the scope of a joint research agreement.

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

Claims 42-59 rejected on the ground of nonstatutory double patenting over claims 1-23 of U. S. Patent No. 6,708,157 and claims 1-45 of USP 7,266,529 since the claims, if allowed, would improperly extend the "right to exclude" already granted in the patent.

The subject matter claimed in the instant application is fully disclosed in the patent and is covered by the patent since the patent and the application are claiming common subject matter, as follows: Rendering digital content in accordance with usage rights information, the usage rights information specifying a manner by which the digital content may be rendered.

Furthermore, there is no apparent reason why applicant was prevented from presenting claims corresponding to those of the instant application during prosecution of

the application which matured into a patent. See *In re Schneller*, 397 F.2d 350, 158 USPQ 210 (CCPA 1968). See also MPEP § 804.

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Behrang Badii whose telephone number is 571-272-6879. The examiner can normally be reached on Monday-Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, James Trammell can be reached on 571-272-6712. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Any response to this action should be mailed to:

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

or faxed to (571)273-8300

Hand delivered responses should be brought to

United States Patent and Trademark Office
Customer Service Window
Randolph Building
401 Dulany Street
Alexandria, VA 22314

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the Technology Center 3600 Customer Service Office whose telephone number is **(571) 272-3600**.

/Behrang Badii/
Primary Examiner, Art Unit 3694



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
11/304,793	12/16/2005	Mark J. Stefik	10-510-US-D6 (cg028300)	6083
98804	7590	06/13/2012	EXAMINER	
Reed Smith LLP P.O. Box 488 Pittsburgh, PA 15230			BADII, BEHRANG	
			ART UNIT	PAPER NUMBER
			3662	
			NOTIFICATION DATE	DELIVERY MODE
			06/13/2012	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

ptoipinbox@reedsmith.com
mskaufman@reedsmith.com

1 UNITED STATES PATENT AND TRADEMARK OFFICE

2
3
4 BEFORE THE BOARD OF PATENT APPEALS
5 AND INTERFERENCES
6

7
8 *Ex parte* MARK J. STEFIK and PETER L. T. PIROLI
9

10
11 Appeal 2011-007642
12 Application 11/304,793
13 Technology Center 3600
14

15
16
17 Before MURRIEL E. CRAWFORD, ANTON W. FETTING, and
18 MICHAEL W. KIM, *Administrative Patent Judges*.
19 FETTING, *Administrative Patent Judge*.

20 DECISION ON APPEAL

STATEMENT OF THE CASE¹

Mark J. Stefik and Peter L. T. Pirolli (Appellants) seek review under 35 U.S.C. § 134 (2002) of a final rejection of claims 42-59, the only claims pending in the application on appeal. We have jurisdiction over the appeal pursuant to 35 U.S.C. § 6(b) (2002).

The Appellants invented a way for associating usage rights with digital content, including creating usage rights from a grammar, the usage rights specifying a manner of use indicating purposes for which the digital content is used and/or distributed by an authorized party; associating the usage rights with a digital content; processing a usage transaction specifying the usage rights to determine if access to the digital content is granted; and storing the usage rights in a distributed repository. The usage rights also specify one or more conditions which must be satisfied before the manner of use is exercised. The creating includes selecting symbols from a first set of predetermined symbols to define a valid sequence of symbols to indicate the manner of use, selecting one or more symbols from a second set of predetermined symbols to define a valid sequence of symbols to indicate the conditions. (Specification ¶ 0016).

An understanding of the invention can be derived from a reading of exemplary claim 42, which is reproduced below [bracketed matter and some paragraphing added].

¹ Our decision will make reference to the Appellants' Appeal Brief ("App. Br.," filed July 13, 2010) and Reply Brief ("Reply Br.," filed January 28, 2011), and the Examiner's Answer ("Ans.," mailed December 3, 2010).

1 42. A computer-implemented method
2 of rendering digital content at a recipient repository in
3 accordance with usage rights information,
4 the method comprising:
5 [1] establishing trust
6 for the purpose of receiving the digital content;
7 [2] after said establishing step,
8 receiving the digital content
9 at the recipient repository;
10 [3] receiving a request
11 at the recipient repository
12 to render the digital content;
13 [4] determining,
14 based on the usage rights information
15 indicating a manner of use
16 by which the digital content may be
17 rendered,
18 whether the content may be rendered
19 in accordance with a specified manner;
20 [5] rendering the digital content
21 in accordance with the specified manner
22 only if it is determined
23 that the content may be rendered
24 in accordance with the specified manner;
25 and
26 [6] denying the request
27 and
28 preventing rendering of the digital content

1 if it is determined that the digital content may not
2 be rendered in accordance with the specified
3 manner.

4 The Examiner relies upon the following prior art:

Wyman	US 5,438,508	Aug. 1, 1995
Pinard	US 5,638,494	Jun. 10, 1997

5 Claims 42-59 stand rejected under 35 U.S.C. § 103(a) as unpatentable
6 over Wyman and Pinard.

7 Claims 42-59 stand rejected under the judicially created doctrine of
8 obvious type double patenting.

9 ISSUES

10 The issues of obviousness turn primarily on the scope of the limitation
11 of “establishing trust.” The issue of double patenting turns primarily on
12 whether the claims attempt to extend the period of protection of claims in
13 issued patents.

14 FACTS PERTINENT TO THE ISSUES

15 The following enumerated Findings of Fact (FF) are believed to be
16 supported by a preponderance of the evidence.

17 *Facts Related to the Prior Art*

18 *Wyman*

19 01. Wyman is directed to managing the licensing of software
20 executed on computer systems. Wyman 1:29-32.

1 02. A license management system is used to account for software
2 product usage in a computer system. Wyman establishes a
3 management policy having a variety of simultaneously-available
4 alternative styles and contexts. A license server administers the
5 license, and each licensed product upon start-up makes a call to
6 the license server to check on whether usage is permitted. The
7 license server maintains a store of the licenses, called product use
8 authorizations, that it administers. Upon receiving a call from a
9 user, the license server checks the product use authorization to
10 determine if the particular use requested is permitted, and, if so,
11 returns a grant to the requesting user node. The license server
12 maintains a database of product use authorizations for the licensed
13 products, and accesses this database for updating and when a
14 request is received from a user. In a distributed system, a license
15 server executes on a server node and the products for which
16 licenses are administered are on client nodes. Wyman 6:48 – 7:4.

17 03. The field 49 contains a calling authorization and/or a caller
18 authorization. If the caller authorization is true, the product is
19 permitted to receive calls from other named products requesting
20 use of the product, and if conditions are met (identified caller is
21 authorized) the server can grant a calling card, as described below.
22 If the calling authorization is true, the product can make calls to
23 other products. If neither is true, then the product can neither
24 make nor receive calls using the calling card feature. The feature
25 of calling cards is important for distributed applications. For
26 example, if a product is able to execute faster in a distributed

1 system by assigning tasks to other CPUs, then the issue is
2 presented of which license policy is needed, i.e., does every node
3 executing a part of the task have to be licensed and consume or
4 receive allocation of a unit, or just the one managing the task?
5 This is resolved for most applications by use of this calling card
6 concept. The product use authorization for such a product has
7 the calling authorization field 49 enabled, so calling cards can
8 be issued. This feature is typically separately priced. Wyman
9 13:14-44.

10 *Pinard*

11 04. Pinard is directed to a communication system which is self
12 adaptive to its users, and both create and provide the services
13 required as needed. The system can be used to manage the flow
14 of work, detect and correct inefficiencies, negotiate service with
15 outside systems, and can be tightly integrated with and adapt to
16 the human based user organization's work processes and goals.
17 Pinard 1:39-45.

18 05. Services can be created dynamically by having a process agent,
19 which has the sole task to create and maintain services. Entities
20 which request new services of processes post their request to an
21 area of a blackboard. A request could come from an agent, as a
22 dynamic request, or from an enterprise modeling tool which has
23 collected via static input a process that needs to be added to the
24 communication system. This spawns a process agent which is
25 responsible for attempting to meet the requested process. The

1 process agent has access to a database which has a digit-tree-like
2 structure made up of pointers to existing agents which can handle
3 various tasks. The process agent reads and interprets this data
4 in order to determine which agents are required to realize the
5 requested service. The process agent then negotiates the usage
6 rights with each of the various agents involved in creating the new
7 process, on pieces needed to create a new process necessary to
8 run the new requested service. The new process agent decides
9 whether or not to install itself in the database of existing
10 processes, in order to become accessible to other agents wanting
11 the same service. The new process agent could also provide itself
12 to the requesting agent, and eliminate itself otherwise. Pinard
13 6:41-68.

14 06. As an example, a user would like to create a new process to
15 handle monthly reports. On finishing the report, the user would
16 like it to automatically be stored in a memory, mailed to a specific
17 mailing list, and have a "to do" list updated. There already exists
18 an agent which handles the sending of ASCII text files to a given
19 user, and there also already exists an agent which is responsible
20 for storing files, and another agent which handles "to do" lists of
21 users. The request of the user is posted to a blackboard; a new
22 process agent is created and given expected inputs from input
23 agents and expected outputs of output agents. The new process
24 agent then negotiates usage rights with the existing agents and
25 puts a procedure together which is comprised of sending a goal to
26 the correct ASCII to Quickmail agent, for each member on the list

1 of users provided, and then sends the file to the storage agent, and
2 makes an update list request to the user's "to do" list agent. Pinard
3 7:1-22.

4 ANALYSIS

5 *Claims 42-59 rejected under 35 U.S.C. § 103(a) as unpatentable over*
6 *Wyman and Pinard.*

7 We are not persuaded by the Appellants' argument that

8 Wyman fails to disclose, suggest, or render obvious
9 "establishing trust for the purpose of receiving the digital
10 content" as is recited in the claims

11 Appeal Br. 7. Wyman clearly describes a license management system
12 that checks whether content usage is permitted. This is uncontested. It is
13 the nature of the recited trust for receiving that content that is contested. As
14 Wyman describes using a license for such receipt, Wyman's system trusts its
15 license system for such receipt. Claim 42 does not narrow the nature of the
16 trust, what content such trust is directed to, and the scope of what portion of
17 a system is to be trusted. Claim 42 simply establishes trust, albeit for some
18 nominal purpose. Appellants appear to be arguing the manner in which such
19 trust occurs, but the claim only calls for establishing the trust. Indeed the
20 limitation "for the purpose of receiving the digital content" is merely
21 aspirational, and the limitation "receiving the digital content at the recipient
22 repository" is not contingent on such trust, but merely subsequent to the step
23 of establishing trust, whatever that is. Thus, Appellants' argument that
24 the "license server", as disclosed in Wyman, does not establish
25 trust between the "requesting user node" and the "license
26 server" receiving the "particular use requested", but rather

1 specifies that the “license server” checks the requested use
2 against the license to determine if the “particular use requested”
3 is permitted

4 (Appeal Br. 8) is simply not commensurate with the scope of the
5 limitation. Such a check at least establishes trust that the check occurred.
6 Appellants next argue that “trust” is defined by purpose. Appeal Br. 9. But
7 a method claim is defined by steps, not purpose.

8 We are not persuaded by the Appellants’ argument that

9 Wyman and Pinard fail to disclose, suggest, or render obvious
10 “determining, based on the usage rights information indicating
11 a manner of use by which the digital content may be rendered,
12 whether the content may be rendered in accordance with a
13 specified manner,” as is recited in the claims.

14 Appeal Br. 10. As the Examiner found at Answer 5, Pinard describes
15 determining such a manner of use with software agents. FF 05-06.

16 As to the nominal arguments of remaining claims, Appellants merely
17 recite various limitations, but base their arguments on those in support of
18 claim 42. Thus these claims fall with claim 42.

19 *Claims 42-59 rejected under the judicially created doctrine of obvious type*
20 *double patenting.*

21 We are persuaded by the Appellants’ argument that the claims of the
22 instant application merely extend the period of coverage of claims in issued
23 patents US 6,708,157 and US 7,266,529. The claims in both of those patents
24 contain limitations that are not in the claims of the instant application. Thus
25 this is not a case of extending a claim to ABCX by claiming ABCXY. *See*
26 *In re Schneller*, 397 F.2d 350 (CCPA 1968).

CONCLUSIONS OF LAW

The rejection of claims 42-59 under 35 U.S.C. § 103(a) as unpatentable over Wyman and Pinard is proper.

The rejection of claims 42-59 under the judicially created doctrine of obvious type double patenting is improper.

DECISION

The rejection of claims 42-59 is affirmed.

No time period for taking any subsequent action in connection with this appeal may be extended under 37 C.F.R. § 1.136(a). *See* 37 C.F.R. § 1.136(a)(1)(iv) (2007).

AFFIRMED

JRG

Electronic Acknowledgement Receipt

EFS ID:	13803237
Application Number:	13585408
International Application Number:	
Confirmation Number:	4941
Title of Invention:	SYSTEM AND METHOD FOR DISTRIBUTING DIGITAL CONTENT TO BE RENDERED IN ACCORDANCE WITH USAGE RIGHTS INFORMATION
First Named Inventor/Applicant Name:	Mark J. Stefik
Customer Number:	98804
Filer:	Stephen M. Hertzler
Filer Authorized By:	
Attorney Docket Number:	10-510-US-C73
Receipt Date:	21-SEP-2012
Filing Date:	14-AUG-2012
Time Stamp:	15:32:53
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	Information Disclosure Statement (IDS) Form (SB08)	10-510-US-C73_-_2012-09-21_-_Information_Disclosure_Statement.pdf	612303 3e64b6a1446dcbedf4a0474c91540dd48d3d4ebbb	no	4

Warnings:

Information:

A U.S. Patent Number Citation or a U.S. Publication Number Citation is required in the Information Disclosure Statement (IDS) form for autoloading of data into USPTO systems. You may remove the form to add the required data in order to correct the Informational Message if you are citing U.S. References. If you chose not to include U.S. References, the image of the form will be processed and be made available within the Image File Wrapper (IFW) system. However, no data will be extracted from this form. Any additional data such as Foreign Patent Documents or Non Patent Literature will be manually reviewed and keyed into USPTO systems.

2	Other Reference-Patent or Application Document	10-510-US-C73_-_2012-09-21_-_Office_Action_from_10-510-US-D6.pdf	335067 0149d6e154fd68d6a5ad6c85cc1fa099badb5613	no	10
Warnings:					
Information:					
3	Other Reference-Patent or Application Document	10-510-US-C73_-_2012-09-21_-_Final_Office_Action_from_10-510-US-D6.pdf	462201 cbc597a2f5d743d7d9f4f7204a2570bec63dee1	no	12
Warnings:					
Information:					
4	Other Reference-Patent or Application Document	10-510-US-C73_-_2012-09-21_-_Office_Action2_from_10-510-US-D6.pdf	566997 71f321abf9e7201b8e779b43348a9f38d7e7dbc4	no	15
Warnings:					
Information:					
5	Other Reference-Patent or Application Document	10-510-US-C73_-_2012-09-21_-_Final_Office_Action2_from_10-510-US-D6.pdf	386250 1386866bffa814390e03aa825c2689433c8f4ca	no	10
Warnings:					
Information:					
6	Other Reference-Patent or Application Document	10-510-US-C73_-_2012-09-21_-_Deciscion_on_Appeal_10-510-US-D6.pdf	363212 17052b9e73a5ad01c2ed7c9d378e6c8a887ef6c1	no	11
Warnings:					
Information:					
Total Files Size (in bytes):			2726030		

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.



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
13/585,408	08/14/2012	Mark J. Stefik	10-510-US-C73

98804
Reed Smith LLP
P.O. Box 488
Pittsburgh, PA 15230

CONFIRMATION NO. 4941
POA ACCEPTANCE LETTER



Date Mailed: 09/26/2012

NOTICE OF ACCEPTANCE OF POWER OF ATTORNEY

This is in response to the Power of Attorney filed 09/17/2012.

The Power of Attorney in this application is accepted. Correspondence in this application will be mailed to the above address as provided by 37 CFR 1.33.

/tnnguyen/

Office of Data Management, Application Assistance Unit (571) 272-4000, or (571) 272-4200, or 1-888-786-0101



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
13/585,408	08/14/2012	Mark J. Stefik	10-510-US-C73

98804
Reed Smith LLP
P.O. Box 488
Pittsburgh, PA 15230

CONFIRMATION NO. 4941
POWER OF ATTORNEY NOTICE



Date Mailed: 09/26/2012

NOTICE REGARDING CHANGE OF POWER OF ATTORNEY

This is in response to the Power of Attorney filed 09/17/2012.

- The Power of Attorney to you in this application has been revoked by the assignee who has intervened as provided by 37 CFR 3.71. Future correspondence will be mailed to the new address of record(37 CFR 1.33).

/tnnguyen/

Office of Data Management, Application Assistance Unit (571) 272-4000, or (571) 272-4200, or 1-888-786-0101

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		13585408
	Filing Date		2012-08-14
	First Named Inventor	Mark J. Stefik	
	Art Unit	2431	
	Examiner Name		
	Attorney Docket Number	10-510-US-C73	

U.S.PATENTS						Remove
Examiner Initial*	Cite No	Patent Number	Kind Code ¹	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	5204961		1993-04-20	Barlow	
	2	4817140		1989-03-28	Chandra et al.	
	3	5390297		1995-02-14	Barber et al.	
	4	6135646		2000-10-24	Kahn et al.	

If you wish to add additional U.S. Patent citation information please click the Add button.

Add

U.S.PATENT APPLICATION PUBLICATIONS						Remove
Examiner Initial*	Cite No	Publication Number	Kind Code ¹	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Published Application citation information please click the Add button.

Add

FOREIGN PATENT DOCUMENTS								Remove
Examiner Initial*	Cite No	Foreign Document Number ³	Country Code ²	Kind Code ⁴	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T ⁵

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		13585408	
	Filing Date		2012-08-14	
	First Named Inventor	Mark J. Stefik		
	Art Unit	2431		
	Examiner Name			
	Attorney Docket Number	10-510-US-C73		

	1	0588415	EP	A1	1994-03-23	Huss, et al.		☐
	2	0398492	EP	A2	1990-11-22	Loucks, et al.		☐

If you wish to add additional Foreign Patent Document citation information please click the Add button **Add**

NON-PATENT LITERATURE DOCUMENTS

Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T ⁵
	1	KOHL, JOHN T. et al., "The Evolution of the Kerberos Authentication Service", Distributed Open Systems, IEEE, 1994, 18 pages.	☐

If you wish to add additional non-patent literature document citation information please click the Add button **Add**

EXAMINER SIGNATURE

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

¹ See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. ² Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). ³ For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. ⁴ Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. ⁵ Applicant is to place a check mark here if English language translation is attached.

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	13585408
Filing Date	2012-08-14
First Named Inventor	Mark J. Stefik
Art Unit	2431
Examiner Name	
Attorney Docket Number	10-510-US-C73

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

☐ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

☐ See attached certification statement.

☐ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Stephen M. Hertzler, Reg. No. 58,247/	Date (YYYY-MM-DD)	2012-09-28
Name/Print	Stephen M. Hertzler	Registration Number	58,247

This collection of information is required by 37 CFR 1.97 and 1.98. 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 1.14. This collection is estimated to take 1 hour 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.**

Privacy Act Statement

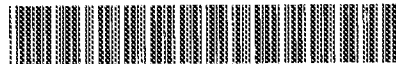
The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these records.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.



Europäisches Patentamt
European Patent Office
Office européen des brevets



Publication number: **0 588 415 A1**

EUROPEAN PATENT APPLICATION

Application number: 93202581.0

Int. Cl.⁵: G06F 1/00, G06F 12/14

Date of filing: 03.09.93

Priority: 11.09.92 US 943654

Date of publication of application:
23.03.94 Bulletin 94/12

Designated Contracting States:
DE FR GB

Applicant: International Business Machines
Corporation
Old Orchard Road
Armonk, N.Y. 10504(US)

Inventor: Carlson, Brent Allen
407 14th Avenue S.W.
Rochester, Minnesota 55902(US)

Inventor: Huss, Frederic Lawrence
1016 21ST Street N.E.
Rochester, Minnesota 55906(US)
Inventor: Schmucki, Nancy Marie
4304 13th Avenue N.W.
Rochester, Minnesota 55901(US)
Inventor: Zelenski, Richard Elmer
529 29th Street N.W.
Rochester, Minnesota 55901-2381(US)

Representative: Louet Feisser, Arnold et al
Trenité Van Doorne
De Laressestraat 133
NL-1075 HJ Amsterdam (NL)

Peer to peer connection authorizer.

A peer to peer connection authorizer is disclosed. The connection authorizer involves three different entities: a system authorizer mechanism, a client connection manager, and a server connection manager. The system authorizer resides on the main or primary CPU while the client and server connection managers reside on individual IOPs. To obtain information required by a user and/or an application program, the client connection manager issues a request to the system authorizer. When the system authorizer receives the request, it first verifies that the client device is who it claims to be. If the system authorizer determines that the client device should be allowed to access the requested information, it then sends a token to the server device and a copy of the same token to the client device. Upon receipt of the token copy from the system authorizer, the client connection manager packages the token copy into a message that it sends to the server device. When the server connection manager receives the message from the client device, it compares the token copy to the token it received from the system authorizer. If the tokens match, the server connection manager responds to the client device and the connection is established.

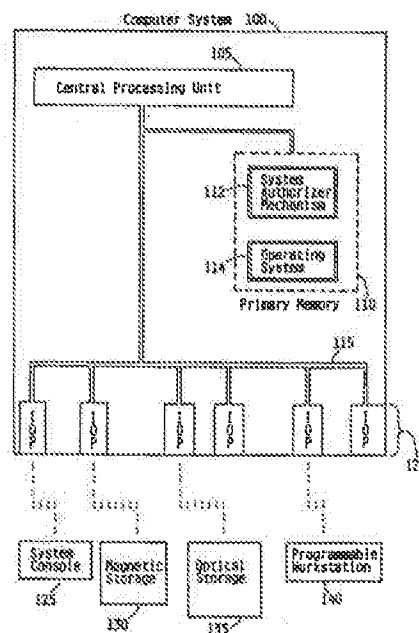


FIG. 1

EP 0 588 415 A1

This invention relates to the data processing field. More specifically, this invention relates to the authorization of peer to peer connections.

Since early computer systems performed only simple tasks, it was unnecessary for them to include more than one input/output unit (I/O unit). For this reason, computer systems such as the EDVAC device of 1948 contained only a single I/O unit. The I/O unit was merely the mechanism used by the computer system to communicate with the outside world. Since these early computer systems required a relatively small amount of information, the I/O unit could be controlled by the central processing unit (CPU) itself. As time passed, the complex tasks performed by computer systems required access to more and more information. Direct control of the I/O unit by the CPU was no longer practical.

In 1959, Univac Corporation introduced its LARC computer system. The LARC computer system included an input/output controller (IOC) which was itself a genuine computer. The IOC was used to handle the flow of information to and from the outside world, thereby reducing the work required of the CPU. While the IOC controlled up to eight I/O channels, modern day computer systems usually include a single I/O controller for each I/O channel. These I/O controllers are called input/output processors (IOPs). Similar to the IOC of the LARC computer system, IOPs are computer systems unto themselves. Each IOP is responsible for handling the information flow between a particular external device (i.e., "the outside world") and the computer system.

The wide use of IOPs has greatly improved the overall performance of today's computer systems. Computer systems can now communicate with a variety of external devices without overly burdening the CPU. Examples of devices which can be connected via IOPs include: terminals, magnetic storage units, optical storage devices, programmable workstations, and other computer systems. To the computer system, each of these external devices represents a resource that can be used to perform a specified task. In many cases, the task to be performed can be accomplished by the external devices without extensive intervention on the part of the CPU. This, of course, greatly reduces the work required of the CPU.

Since today's multimedia applications typically require extensive access to audio and video information, they are illustrative of the potential performance advantage of IOPs. The amount of data necessary to present a user with audio and video information is enormous. Hence, tremendous performance savings are possible in theory by allowing a multimedia application associated with an IOP to bypass the main CPU and access information

from another IOP directly. Inherent in this noninterventionist approach, however, is the problem of securing information and resources. Allowing external devices to connect at will makes unauthorized use of system resources a real problem. Without some type of security, the users associated with the various external devices may attempt to gain access to personal or otherwise sensitive information. This problem is magnified when one considers that the computer system, the various IOPs, and the attached external devices may be owned or manufactured by different parties. In this later, worse case scenario, rogue IOPs may actually be introduced into the computer system to facilitate the unauthorized use of system resources (i.e., to steal information).

Solutions to this problem invariably involve some CPU intervention. Thus a balance is struck between efficiency and security. A computer system which is more secure tends to be less efficient while a computer system which is very efficient tends to be less secure. This tradeoff stems from the fact that highly secure computer systems must include a means (i.e., authorization means) to allow or disallow access to system resources. While authorization means do provide for increased security, they also create expensive performance overhead which reduces overall system efficiency. Hence, computer system designers are always attempting to design systems that are efficient yet secure (i.e., "to have their cake and eat it too").

A solution to a related security problem is an authorization model called Kerberos. Kerberos was jointly developed by Digital Equipment Corporation, International Business Machines Corporation (IBM), and the Massachusetts Institute of Technology (MIT) for use on an MIT campus-wide computer network.

Kerberos uses a system of messages and keys to deal with the security problem. To obtain information from a server device, a client device must first request authorization from a Kerberos server. This action triggers a series of encrypted messages which are sent by the Kerberos server to the client and server devices and from the client device to the server device. Eventually, the client device is able to connect to the server device.

Although Kerberos is an illustrative solution to a related security problem, Kerberos was not designed to solve the problem of rogue IOPs. Further, the Kerberos authentication model is itself flawed in many respects. One problem with the Kerberos model is its inherent complexity. Each device that wishes to participate in the authentication scheme must first register itself with the appropriate Kerberos server. To accomplish this, the subject device must first have knowledge about the resources controlled by particular Kerberos servers and then

register with the appropriate Kerberos server or servers. The registration process is itself complex in that each Kerberos server must allocate a unique encryption key to each device. If multiple Kerberos servers are involved, each device must understand what key is to be used for what resources.

The inherent complexity of the Kerberos model is exacerbated by the model's dependence on encryption. The Kerberos model would simply not work without its elaborate system of key based encryption. Each device must support shared secret key cryptography and understand how the keys are used within the Kerberos protocol. When a Kerberos client device receives an authorization request, it must know what key is to be associated with the client device, what key is to be associated with the server device, and what unique key can be used to communicate between the two devices. When the client device receives this information from the Kerberos server, it must understand that it needs to use its key to decrypt the message sent to it, that it cannot decrypt the message sent from the Kerberos server to the server device, and that it must use the new key to encrypt its response message to the server device. When the server device finally gets the message from the client device, it must understand that it needs to use its shared secret key to access the new key and that it must use the new key to access the information from the client device. This complexity is compounded when one remembers that each device can be involved in multiple connections.

Yet another problem with the Kerberos model and generally the noninterventionist approach, is the lack of resource information available to client devices. Beyond the need to understand the location of system resources for registration purposes, each client must expressly inform the Kerberos server of the name of the particular server device with which it wishes to communicate. The Kerberos model does not contemplate authorization on an entity to information basis. In other words, a client device cannot simply say "I want access to information X." A Kerberos server would reject such a request as lacking the appropriate server address information.

It is a principal object of this invention to provide an enhanced method and apparatus for communicating data among the components of a computer system.

It is another object of this invention to provide an enhanced method and apparatus for authorizing connections among the IOPs of a computer system.

It is yet another object of this invention to provide an enhanced method and apparatus for authorizing connections among like entities.

It is still another object of this invention to provide an enhanced method and apparatus for authorizing connections between a server entity and a plurality of client entities.

It is still another object of this invention to provide an enhanced method and apparatus for authorizing connections between a plurality of server entities and a single client entity.

It is still another object of this invention to provide an enhanced method and apparatus for authorizing connections between a plurality of server entities and a plurality of client entities.

It is still another object of this invention to provide an enhanced method and apparatus for preventing rogue IOPs from accessing system resources.

These and other objects are accomplished by the peer to peer connection authoriser disclosed herein.

Conceptually, the authorization technique used by the disclosed peer to peer connection authorizer involves three different entities: a system authorizer mechanism, a client connection manager, and a server connection manager. The system authorizer resides on the main or primary CPU while the client and server connection managers reside on individual IOPs.

To obtain information required by a user and/or an application program, the client connection manager issues a request to the system authorizer. Since the client application may or may not know the location of the desired information, the request may or may not include the address of a server device (i.e., the client connection manager will not provide the address of a server device when the location of the information is unknown to it). When the system authoriser receives the request, it first verifies that the client device is who it claims to be. The system authorizer then identifies the applicable server device by using either the address provided by the client connection manager or the information contained in the request. If the system authorizer determines that the client device should be allowed to access the information on the subject server device, it then sends a token to the server device and a copy of the same token to the client device. Depending on security needs, the token may or may not be encrypted. It is also possible that the requisite information resides on more than one server device or that more than one client device requires the information. The system authoriser handles multiple device situations by dispatching multiple tokens and token copies.

Upon receipt of the token copy from the system authorizer, the client connection manager packages the token copy into a message that it sends to the server device. When the server connection manager receives the message from the

client device, it compares the token copy to the token it received from the system authorizer. If the tokens match, the server connection manager responds to the client device and the connection is established. If the tokens do not match, the server connection manager notifies the system authorizer of the failed connection attempt and then proceeds to inform the client device.

Brief description of the drawings:

Fig. 1 shows the computer system of the present invention.

Fig. 2 shows the IOPs and the connection managers of the present invention.

Fig. 3 shows a high level functional diagram of the message flow between the system authorizer and the client and server IOPs of the present invention.

Fig. 4 shows block diagrams of the request message and the authorization and authorization response messages of the preferred embodiment.

Fig. 5 shows block diagrams of the open and open response messages of the preferred embodiment.

Fig. 6 shows block diagrams of the open, unauthorized open attempt, cancel token, and open response messages of the preferred embodiment.

Fig. 7 shows a block diagram of the format of the token of the preferred embodiment.

Fig. 8 shows a logic flow diagram of the system authorizer mechanism of the present invention.

Fig. 9 shows a logic flow diagram of the server IOP connection manager of the present invention.

Fig. 10 shows a logic flow diagram of the client IOP connection manager of the present invention.

Fig. 1 shows a block diagram of the computer system of the present invention. The computer system of the preferred embodiment is an IBM AS/400 mid-range computer system. However, any computer system could be used. Fig. 1 shows an exploded view of computer system 100. Computer system 100 comprises main or central processing unit (CPU) 105 connected to primary memory 110 and system I/O bus 115. Although the system depicted in Fig. 1 contains only a single main CPU and a single system I/O bus, it should be understood that the present invention applies equally to computer systems having multiple main CPUs and multiple I/O buses. Similarly, although the I/O bus of the preferred embodiment is a typical hardwired, multidrop bus, any connection means that supports bi-directional communication could be used.

Connected to system I/O bus 115 are IOPs 120. Although Fig. 1 shows six IOPs and four external devices, it should be understood that the present invention applies equally to any number of external devices connected to any number of IOPs.

Each of IOPs 120 is designed to communicate with bus 115 and the external device for which it is responsible. The processors used in the IOPs of the preferred embodiment (IOPs 120) are Motorola 68020 micro computers, but other micro computers, such as the Intel 960, could be used. System console 125 is connected to bus 115 via one of the IOPs 120. System console 125 allows system administrators to communicate with computer system 100, normally through a non-programmable workstation. Similarly, magnetic storage 130, optical storage 135, and programmable workstation 140 are each connected to bus 115 via one of IOPs 120. Secondary storage devices 130 and 135 (i.e., magnetic storage 130, and optical storage 135) are used by computer system 100 as large storage repositories for data and programs. Programmable workstation 140 allows users and developers to communicate with computer system 100.

Primary memory 110 contains system authorizer mechanism 112 and operating system 114. System authorizer 112 is shown to reside in primary memory 110. However, it should be understood that while system authorizer 112 will typically be loaded into primary memory to execute, it may at some point reside in magnetic storage 130 or optical storage 135.

Fig. 2 shows an exploded view of two of IOPs 120. As shown, IOPs 200 and 250 are used as interfaces between I/O bus 115 and devices 230 and 260. Focusing on IOP 200, Fig. 2 shows that CPU 210, bus interface 205, primary memory 215 and device interface 220 are all interconnected via bus 225. Residing in primary memory 215 is IOP connection manager 217.

While in many cases bus interface 205, CPU 210, primary memory 215, and bus 225 are the same in each of IOPs 120, IOP connection manager 217 and device interface 220 are usually device dependent. In other words, IOP connection manager 217 and device interface 220 may vary depending upon the nature of device 230. For example, if device 230 is a magnetic storage device, IOP connection manager 217 will usually be a server connection manager and device interface 220 will comprise input/output hardware commensurate with the magnetic storage device. If, in contrast, device 230 is a programmable workstation (PWS), IOP connection manager 217 will be a client connection manager and device interface 220 will similarly comprise input/output hardware commensurate with the PWS.

Fig. 3 shows a functional flow diagram of the interaction between system authorizer 112 and server connection manager 300 and client connection manager 350. Two different types of logical connections are shown on Fig. 3. Services connections 320, 370, and 385 are used to pass connec-

tion oriented information while data connection 390 is used for data transmission. Although in the figures these connections appear as logical connections, it should be understood that these connections physically take place on I/O bus 115. In the preferred embodiment, the IBM Inter-process Communication Facility (IPCF) protocol is used to establish these logical connections. However, any protocol capable of creating logical connections could be used. For more information about the IPCF protocol, refer to U.S. Patent 4,649,473 to Hammer et. al which is included herein by reference.

The names and locations of all of the IOPs are made known to system authorizer mechanism 112 as part of the initialization sequence for computer system 100. Similarly, the bus address and name of system authorizer mechanism 112 are made known to each of the IOPs. The need for authorization first occurs when an application running on client device 380 requires access to resources that exist on a different device. Client connection manager 350 begins the authorization process by sending request message 360 to system authorizer mechanism 112 via services connection 370. Request message 360 may indicate that a connection to a specific server IOP is desired or it may simply request access to particular information.

System authorizer mechanism 112 reacts to request message 360 by sending Peer to Peer Authorization message (hereafter PTPA message) 322 to server connection manager 300 via services connection 320. The format of PTPA message 322 is shown on Figure 4. Although the fields and format of this message will be described in greater detail in the discussion associated with Figures 8-10, it is important to note the existence of server token 440. Server token 440 will be used later in the authorization process to determine whether server connection manager 300 should comply with an open request from a client connection manager. It is also important to note that server connection manager 300 only accepts tokens that are supplied by system authorizer mechanism 112.

After receipt of PTPA message 322, server connection manager 300 uses services connection 320 to respond to system authorizer mechanism 112 with Authorization Response (AR) message 324. If all is well with AR message 324, system authorizer mechanism 112 uses services connection 370 to send Open Peer to Peer System to IOP message (hereafter OPTPSTI message) 374 to client connection manager 350. The format of OPTPSTI message 374 is shown on Fig. 5. Although the fields and format of this message will be described in greater detail in the discussion associated with Figs. 8-10, it is important to note the existence of server copy token 525. Server copy

token 525 is used by client connection manager 350 to validate its resource request with server connection manager 300. Client connection manager 350 bundles server copy token 525 into Open Peer to Peer IOP to IOP message (hereafter OPTPITI message) 375 and sends the message to server connection manager 300 via services connection 385. (The format of OPTPITI message 374 is shown on Fig. 6.)

Upon receipt of OPTPITI message 375, server connection manager 300 compares server copy token 615 to server token 440. If the tokens match, server connection manager 300 sends Open Peer to Peer IOP to IOP response message (hereafter OPTPITIR message) 325, via services connection 385, to inform client connection manager 350 that access has been authorized. The data connection is then set up over data connection 390.

If the tokens do not match, server connection manager 300 informs system authorizer 112 of the invalid access attempt by sending Unauthorized Open Attempt message (hereafter UOA message) 310 via services connection 320. After dispatching this message, server connection manager 300 sends OPTPITIR message 325, via services connection 385, to inform client connection manager 350 that its access attempt has been rejected.

When system authorization mechanism 112 receives an UOA message, it has the responsibility of taking appropriate action. The appropriate action may range from "doing nothing" to sending a Cancel Token message (hereafter CT message) to server connection manager 350. The CT message is a command which effectively tells server connection managers to refrain from accepting access attempts that are associated with the subject token.

Upon receipt of OPTPITIR message 325, client connection manager 350 is required to inform system authorizer 112 of the outcome of the access attempt. To do so, client connection manager 350 sends Open Peer to Peer System to IOP Response message (hereafter OPTPSTIR message) 360 to system authorizer 112 via services connection 370.

Figs. 4-6 show the formats used for the messages of the preferred embodiment. These formats are described in detail in connection with the following discussion of Figs. 8-10.

Fig. 8 shows a flow diagram of the steps taken by system authorizer mechanism 112 to authorize peer to peer connections. For the purposes of explanation, assume that client device 380 of Fig. 3 is a PWS running a multimedia application and that server device 340 of Fig. 3 is an optical storage device. Further assume that optical storage device 340 contains multimedia information that is required by the multimedia application running on PWS 380 and that client and server connection managers 350 and 300 of Fig. 3 are running on the

IOPs associated with PWS 380 and optical storage device 340 respectively.

In block 800, system authorizer mechanism 112 obtains and stores in an appropriate table the names and locations of all the IOPs of computer system 100. As stated, this is accomplished as part of the initialization of computer system 100.

After initialization in block 800, system authorizer mechanism 112 waits for authorization requests 806. System authorizer mechanism 112 will return to this wait state whenever processing of an authorization request has been completed. Blocks 805 and 810 represent two different types of authorization requests. External authorization request 810 represents a request that originated in a device external to computer system 100. In the case at hand, the external request originated with multimedia PWS 380. Internal authorization request 805 represents a request that is system initiated. This latter request will be described in connection with the discussion of the first alternate embodiment.

When the multimedia application running on PWS 380 requires multimedia information, it will cause client connection manager 350 to send a request message to system authorizer mechanism 112.

Fig. 4 shows the format of the request message. This is the format that is used, for example, in request message 360. Request message format 400 comprises client resource ID field 410, server resource ID field 415, information ID field 420, and access rights field 425. Client resource ID field 410 is used to identify the client device that requires the information. In our multimedia example, the identity of PWS 380 would be contained in this field. Server resource ID field 415 is an optional field that contains location information about the server device. This field could be included in the message if the location of the requested information is known to the client device. In our example, this field would be included if the multimedia application knew that the information it needed was stored on optical storage device 340. Information ID field 420 is used to identify the information or when the locate of that information is unknown to the requestor. For example, the multimedia application running on PWS 380 may know what information it needs, but not where the information is located. In this case, system authorization mechanism 112 uses information ID field 420 to determine the whereabouts of the requested information. In the preferred embodiment, a table (not shown) which correlates particular information IDs to the location of the information is used; however, any means for associating a request for particular information to the location of that information could be used. Access rights field 425 indicates what

type of access the client device requires. For example, the multimedia application running on PWS 380 may want to be authorized to write to as well as read from a particular storage device.

System authorizer mechanism 112 will receive this request in functional block 810. Based on the nature of the request and general system factors, system authorizer mechanism 112 will determine the type of token, the number of tokens sent out, and the distribution of token types 815. General system factors may include current system resource utilization, the location of the information, or any other factor that may affect how the request is processed. Blocks 820, 825, and 830 show the three different types of tokens that can be used. If system authorizer mechanism 112 chooses the single-use token type (shown as choice 830), the token or tokens that are sent out to the server or servers are used once and then destroyed. In our multimedia example, system authorizer mechanism 112 elects to use this token type when, based on the request from client connection manager 350, it determines that all the information could be obtained with a single access. In other words, system authorizer mechanism 112 may determine that the quantity or nature of the requested information is such that it may be retrieved without multiple access requests.

To expand on this example, further assume that some of the requested information was located on optical storage device 340, but that the remaining information was located on another optical storage device (not shown). In the multimedia example, this may occur if the video information were stored on optical storage device 340 and the audio information were stored on another optical storage device (not shown). When this is the case, system authorizer mechanism 112 sends single use tokens to server connection manager 300 and the server connection manager associated with the second optical storage device (not shown). The manner in which these tokens are later used by the subject client connection manager(s) is described in forthcoming paragraphs.

Reusable tokens (shown as choice 825) are used when system authorizer mechanism 112 determines that continued access to the information is required. In our example, system authorizer mechanism 112 may determine from the information supplied by client connection manager 350 that the multimedia application running on PWS 380 will require continued access to the information stored on optical storage device 340. Once again, the example is expanded by assuming that continued access to information stored on an additional optical storage device (not shown) is also required. If this were the case, system authorizer mechanism 112 would send reusable tokens to server connec-

tion manager 300 and the server connection manager associated with the second optical storage device (not shown).

The choice between a single-use token and a reusable token may also involve a tradeoff between security and performance. System authorizer mechanism 112 may choose to use a single access token over a reusable token when the information requested is sensitive in nature. Similarly, system authorizer mechanism 112 may choose to use a reusable token over a single-use token when overall system performance is a primary concern.

The last type of token, the generic token (shown as choice 820), is used to allow free access to the information on a particular server device. In our multimedia example, this may occur if system authorizer mechanism 112 determines that client devices other than PWS 380 will likely be in need of the information stored on optical storage device 340 and that such access should be freely granted. Once again, system authorizer mechanism 112 could determine that these conditions exist for more than just optical storage device 340 and send out multiple generic tokens.

As above, system authorizer mechanism 112 may also elect to use a generic token over the other types of tokens because of system performance concerns.

The encryption option (shown as decision block 835) is included in the preferred embodiment to provide additional security if required. It is important to note, however, that the present invention does not rely on the presence of encryption capability to perform its authorization function. As shown on Fig. 8, the encryption option does not make sense when generic tokens have been chosen.

Once the requested information has been located and the token or tokens of a particular type have been created (and possibly encrypted), system authorizer mechanism 112 bundles it/them into a PTPA message and sends the message(s) to the subject server connection manager(s). Figure 4 shows the format of the PTPA message in more detail. Field 430 contains the PTPA message type indicator.

Field 435 is used within the IPCF protocol to identify the entity for which the authorization is intended. Client access field 450 is used to indicate to the receiving server connection manager (here, server connection manager 300) what access rights have been requested by the client. Field 440 contains the actual token itself while field 445 contains the token type. Token qualifier field 445 contains an indication of the particular token's type (i.e., single use, multiple use, or generic). Fig. 7 shows the token format used in the preferred embodiment. Token format 700 comprises client IOP ad-

dress 705, client IOP resource 710, time of day 715, and random value 720. Client IOP address 705 is a field which contains the location of the client IOP. In our multimedia example, this field would contain the address of the IOP that is running client connection manager 350. Client IOP resource 710 is a field which contains the identification of the resource that is requesting the information. In our example, this field would contain the identification of PWS 380. Time of day field 715 and random value 720 are used for uniqueness and encryption purposes should additional security be required.

In our example, the token would be sent to server connection manager 300 and perhaps others 845. Once this is accomplished, system authorizer mechanism 112 will determine whether the nature of the request and/or general system factors require the use of another token type 850. This scenario can be best explained by reconsidering our expanded multimedia example. Beyond assuming that the required information is located on more than one server device, assume further that the access needs for the server devices are different. For example, the multimedia application may need continuous access to the video information stored on optical storage device 340, but only a single access to the audio information stored on the other optical storage device (not shown). If this were the case, system authorizer mechanism 112 would elect to send a reusable token to server connection manager 300 and a single-use token to the server connection manager (not shown) associated with the other optical storage device (not shown).

When all of the PTPA messages have been dispatched, system authorizer mechanism 112 will begin processing the AR messages that it has received 855. The format of the AR message is shown on Fig. 4. AR format 470 comprises message type field 455 and status field 460. Status field 460 is used by system authorizer 112 to determine whether it is appropriate to proceed. For example, it would not be appropriate to continue if status field 460 indicated that optical storage device 340 was currently unavailable.

Assuming that all is well, system authorization mechanism 112 will proceed to build the necessary OPTPSTI message(s) at step 860. The format of the OPTPSTI message is shown on Fig. 5. OPTPSTI message format 500 comprises message type field 505, client resource ID field 510, server resource ID field 515, server route field 520, server copy token 525, and client access field 530. Client resource ID field 510 identifies the client device for which the authorization is intended. In our case, PWS 380 has made the request and is, therefore, the client device which has been authorized to access the information stored on optical storage

device 340. Server route field 520 contains location information that is used by client connection manager 350 to initiate the connection between PWS 380 and optical storage device 340. Server copy token field 525 contains the copy of the token that must be used to gain access to the information stored on optical storage device 340. Lastly, client access field 530 is used to inform client connection manager 350 of the access rights that have been authorized.

When the appropriate message(s) has been created, it is sent to client connection manager 350 in block 865. At this point, system authorizer mechanism 112 waits to get a response back from client connection manager 350 in block 870. Fig. 5 shows the format of the OPTPSTIR message. OPTPSTIR message format 550 comprises message type field 555, client status field 560, and server status field 565. The status field in each message is used to indicate the status of the subject device. The status fields are processed in block 880 of Fig. 8. If the authorized connection took place, the status fields will so indicate. (The manner in which connections are made is described in the discussion of Figs. 9-10.) If a connection did not take place, the fields will cause system authorizer mechanism 112 to take remedial action (not shown). This remedial action could range from "doing nothing" to canceling the appropriate tokens.

The manner in which system authorizer mechanism 112 processes the UOA message (shown in block 890) will be described in connection with the discussion of Fig. 9.

Fig. 9 shows the process flow for server connection manager 300. In the description of Fig. 8, block 845, we saw that the PTPA message(s) were sent from system authorizer 112 to server connection manager 300. (Refer to the discussion of Fig. 8 for a detailed description of the format of the PTPA message.) Server connection manager 300 receives this message(s) in functional block 900 and proceeds to process the message(s) in block 970. In block 975, server connection manager 300 determines whether it is possible to process the request associated with the message(s). It may not be possible if, for example, optical storage device 340 was inoperable at the time of the request or if the IOP itself did not have enough resources to process the request. If this were the case, connection manager 300 would so indicate in its AR message to system authorizer mechanism 112 (shown by blocks 975 and 942) and complete 932. (Refer to the discussion of Fig. 8 for a detailed description of the format of the AR message.) If it is appropriate for server connection manager 300 to continue, the encryption option is dealt with (shown by blocks 980 and 952) and the token is stored 985. Server connection manager 300 will

then send the appropriate AR message back to system authorizer mechanism 112 (shown by block 980) and complete 962.

Refer now to Fig. 10. (The remaining blocks of Fig. 9 relate to processing that is associated with messages that are sent by client connection manager 350 and system authorizer mechanism 112. These blocks are better understood when the origin of these messages has been explained.) Fig. 10 shows that the OPTPSTI message from system authorizer 112 is received by client connection manager 350 in block 1000. Client connection manager 350 responds to the OPTPSTI message from system authorizer 112 by creating and sending an OPTPITI message to server connection manager 300. Fig. 6 shows the format of the OPTPITI message. OPTPITI message 600 comprises message type 605, server resource ID 610, and server copy token 615. Server resource ID field 610 is used to identify the resource which contains the required information. Server copy token field 615 contains the copy token that was received from system authorizer 112.

Referring back to Fig. 9, the OPTPITI message is received by server connection manager 300 in block 920. After dealing with optional encryption (shown by blocks 945 and 960), server connection manager 300 determines whether the copy token that it received in the OPTPITI message is valid 950. The validation is performed by comparing the copy token to the token that was received in the PTPA message. If the token is valid, server connection manager 300 next asks whether it is appropriate to continue processing the request 963. As above, connection manager 300 is concerned with whether the IOP and the device have enough resources to process the request associated with the token. After the token's validity and the availability of resources have been ensured, server connection manager 300 determines whether the token is a single use token 965. If the token is a single use token, it is destroyed 992 by deleting it from IOP storage. After this decision has been made, server connection manager 300 responds to client connection manager 350 with a OPTPITIR message 962. Fig. 6 shows the format of a OPTPITIR message. OPTPITIR message 650 comprises message type field 620, transfer limits field 625, status field 630, and client access field 633. Transfer limits field 625 will contain such information as the maximum size of message packets and the maximum speed at which they can be transmitted. Status field 630 is used to inform client connection manager 350 of the outcome of the open attempt. As above, client access field 633 is used to inform client connection manager 350 of the access rights that have been authorized.

If server connection manager 300 determines that the copy token is invalid, it will send an UOA message to system authorizer 112 (shown by block 955) before responding to client connection manager 350. Fig. 6 shows the format of the UOA message. UOA message 655 comprises message type field 635, client resource ID field 640, client route field 643, the token that was used in the attempt 645 (i.e., the token contained in server copy token field 615 of the subject OPTPITI message), and time of day field 660. The client resource ID field identifies the client device and the client IOP that are responsible for the rejected open attempt. In our multimedia example this would be PWS 360 and the associated IOP (identified by client route field 643). This message is then processed by system authorizer mechanism 112 in block 890 of Fig. 8. As stated, system authorizer mechanism 112 must determine what remedial action is required. If system authorizer mechanism 112 decides to cancel the valid token, it will send a CT message (not shown) to server connection manager 300. Fig. 6 shows the format of the CT message. CT message format 675 comprises message type field 665, the token to be cancelled 670, and the client route that is associated with the token to be cancelled 673. This message is received by server connection manager 300 in block 925 of Fig. 8. Server connection manager 300 responds to the CT message by destroying the token 930 for the specified IOP. Server connection manager 300 then completes processing 940.

Referring lastly to Fig. 10, client connection manager 350 will receive the OPTPITIIR message from server connection manager 300 in block 1015. If the status field of the OPTPITIIR message indicates that a connection has been authorized, client connection manager 350 will initiate the authorized data connection 1015 and send an OPTPSTIR message 1020 to system authorizer mechanism 112 to notify it of such. If the OPTPITIIR message indicates that a connection has not been authorized, client connection manager 350 must nevertheless use an OPTPSTIR message to notify system authorizer mechanism of the failed attempt. Although this action is required of the client IOP, a rogue client IOP that does not comply with the requirement will not go undetected. As mentioned above, the server connection manager also has the responsibility of notifying the system authorizer (see block 955 of Fig. 9).

In the first alternate embodiment, system authorizer mechanism 112 receives the authorization request internally from computer system 100 itself 805. This would occur when an application running on CPU 105 determined that the devices associated with two or more IOPs should work

together to achieve a particular task. At this point the authorization process would continue as has been described above.

In the second alternate embodiment, the present invention is applied to a network of computers. It should be understood that while the preferred embodiment uses the present invention to authorize connections between the IOPs of a single computer system, the present invention can also be used in a network environment. In this alternate embodiment, IOPs 120 are replaced by one or more independent computers and bus 115 is replaced one or more physical networking interfaces. Examples of such interfaces include: IEEE 802.5 (Token Ring), IEEE 802.4 (Token Bus), IEEE 802.3 (Ethernet), FDDI, X.25, and ISDN. The methods and apparatus described in the primary and first alternate embodiment apply equally to this embodiment.

Although a specific embodiment along with certain alternate embodiments have been disclosed, it will be understood by those skilled in the art that additional variations in form and detail may be made within the scope of the following claims.

Claims

1. A method for communicating data, said method comprising the steps of:
 - requesting access to system resources, said access being requested by a first connection manager, said first connection manager residing on a first IOP;
 - sending an authorization token in response to said requesting step, said authorization token being sent from a system authorizer mechanism to a second IOP connection manager, said second IOP connection manager residing on a second IOP, said authorization token being sent as part of a first message, said first message being transmitted on a bus;
 - sending a copy of said authorization token from said system authorizer to said first IOP connection manager, said authorization token being sent as part of a second message, said second message being transmitted on said bus;
 - requesting a connection with said first IOP connection manager, said connection being requested via a third message, said third message comprising said copy of said token, said third message being transmitted via said bus;
 - validating said copy of said authorization token, said copy of said authorization token being validated by said second IOP connection manager;

- establishing a connection between said first and said second IOPs across said bus based on the outcome of said validating step. 5
- 2. The method of claim 1 wherein said sending an authorization token step comprises at least one of the following steps:
 - sending a generic authorization token;
 - sending a reusable authorization token; 10
 - sending a single-use authorization token;
 - encrypting said authorization token;
 - sending said authorization token to a first server IOP connection manager and to a second server IOP connection manager. 15
- 3. A method for communicating data between a client entity and a server entity, said method comprising the steps of:
 - issuing a request for data; 20
 - receiving in conjunction with said request an authorization token, said authorization token being received at said server entity, said authorization token being sent from an authorizer entity; 25
 - sending a copy of said authorization token from said authorizer entity to said client entity;
 - requesting a connection, said connection being requested via a message sent from said client entity to said server entity, said message comprising a copy of said authorization token; 30
 - validating said copy of said authorization token, said copy of said authorization token being validated by said server entity; 35
 - establishing a connection between said server entity and said client entity when said authorization token has been validated. 40
- 4. The method of any of the preceding claims wherein said sending a copy of said authorization token step comprises at least one of the following steps: 45
 - encrypting said copy of said authorization token;
 - sending said copy of said authorization token to a first client connection manager and to a second client connection manager; 50
 - sending said copy of said authorization token to a first client entity and a second client entity. 55
- 5. A method for communicating data, said method comprising the steps of:
 - issuing a request for data; 10

- receiving in conjunction with said request an authorization token, said authorization token being received at a client entity, said authorization token being sent from an authorizer entity;
 - requesting a connection between said client entity and a server entity, said connection being requested via a first message sent from said client entity to said server entity, said message comprising said authorization token;
 - establishing a connection between said client entity and said server entity based on a response received as a result of said requesting step.
6. The method of any of the preceding claims wherein said establishing step comprises at least one of the following steps:
 - reporting the outcome of said validating step to said client IOP connection manager;
 - reporting the outcome of said validating step to said system authorizer;
 - reporting the outcome of said validating step to said client entity;
 - reporting the outcome of said validating step to said authorizer entity.
7. A method for communicating data between a client entity and a server entity, said method comprising the steps of:
 - receiving in conjunction with a request for data a first authorization token, said authorization token being received at said server entity, said authorization token being sent from an authorizer entity;
 - validating a second authorization token, said validation being done by comparing said second authorization token with said first authorization token, said second authorization token being received as part of a request to establish a connection between said server entity and said client entity.

- 8. The method of any of the preceding claims wherein said receiving step comprises at least one of the following steps:
 - encrypting said authorization token;
 - receiving said authorization token at a first server entity and at a second server entity;
 - receiving a generic authorization token;
 - receiving a reusable authorization token;
 - receiving a single-use authorization token.

9. The method of any of the preceding claims wherein said validating step comprises at least one of the following steps:

- encrypting said authorization token;
- decrypting said authorization token;
- decrypting said authorization token and said copy of said authorization token.

10. An apparatus for communicating data, said apparatus comprising:

- means for requesting access to system resources, said access being requested by a first connection manager, said first connection manager residing on a first IOP;
- means for sending an authorization token in response to said requesting step, said authorization token being sent from a system authorizer mechanism to a second IOP connection manager, said second IOP connection manager residing on a second IOP said authorization token being sent as part of a first message, said first message being transmitted on a bus;
- means for sending a copy of said authorization token from said system authorizer to said first IOP connection manager, said authorization token being sent as part of a second message, said second message being transmitted on said bus;
- means for requesting a connection with said first IOP connection manager, said connection being requested via a third message, said third message comprising said copy of said token, said third message being transmitted via said bus;
- means for validating said copy of said authorization token, said copy of said authorization token being validated by said second IOP connection manager;
- means for establishing a connection between said first and said second IOPs across said bus based on the outcome of said validating step.

11. The apparatus of claim 36 wherein said means for sending authorization token comprises at least one of the following means:

- means for sending a generic authorization token;
- means for sending a reusable authorization token;
- means for sending a single-use authorization token.

12. An apparatus for communicating data between a client entity and a server entity, said apparatus comprising:

- means for issuing a request for data;
- means for receiving in conjunction with said request an authorization token, said authorization token being received at said server entity, said authorization token being sent from a authorizer entity;
- means for sending a copy of said authorization token from said authorizer entity to said client entity;
- means for requesting a connection, said connection being requested via a message sent from said client entity to said server entity, said message comprising a copy of said authorization token; means for validating said copy of said authorization token, said copy of said authorization token being validated by said server entity;
- means for establishing a connection between said server entity and said client entity when said authorization token has been validated.

13. An apparatus for communicating data, said apparatus comprising:

- means for issuing a request for data;
- means for receiving in conjunction with said request an authorization token, said authorization token being received at a client entity, said authorization token being sent from an authorizer entity;
- means for requesting a connection between said client entity and a server entity, said connection being requested via a first message sent from said client entity to said server entity, said message comprising said authorization token;
- means for establishing a connection between said client entity and said server entity based on a response received as a result of said requesting step.

14. The apparatus of any of the preceding claims wherein said means for establishing comprises at least one of the following means:

- means for reporting the outcome of said means for validating to said client IOP connection manager;
- means for reporting the outcome of said means for validating to said system authorizer;
- means for reporting the outcome of said validating step to said authorizer entity;

15. An apparatus for communicating data between a client entity and a server entity, said apparatus comprising:

- means for receiving in conjunction with a request for data a first authorization token, said authorization token being received at said server entity, said authorization token being sent from an authorizer entity; 5
- means for validating a second authorization token, said validation being done by comparing said second authorization token with said first authorization token, said second authorization token being received as part of a request to establish a connection between said server entity and said client entity. 10 15

16. The apparatus of any of the preceding claims wherein said means for receiving comprises at least one of the following means: 20

- means for receiving a generic authorization token;
- means for receiving a reusable authorization token; 25
- means for receiving a single-use authorization token;

30

35

40

45

50

55

12

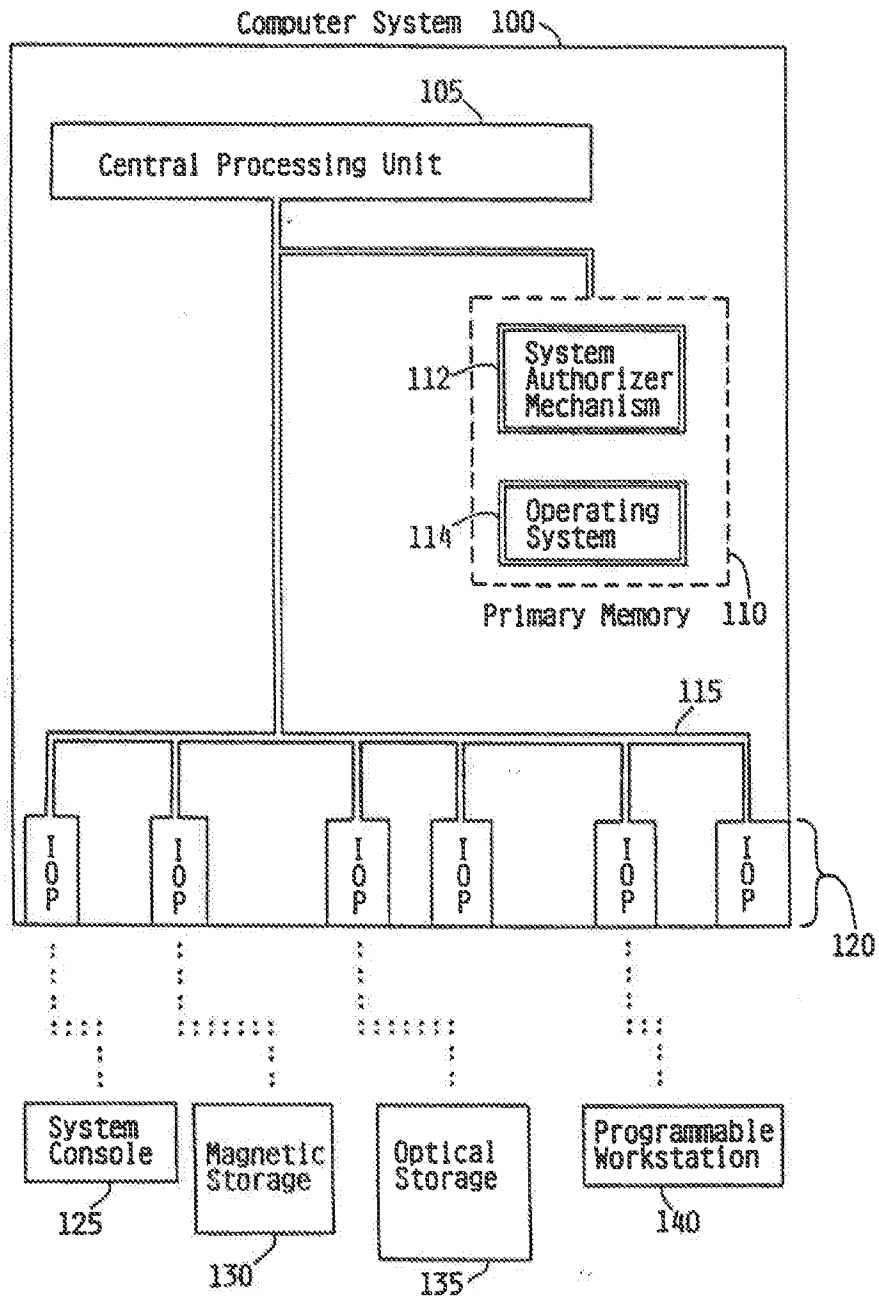


FIG. 1

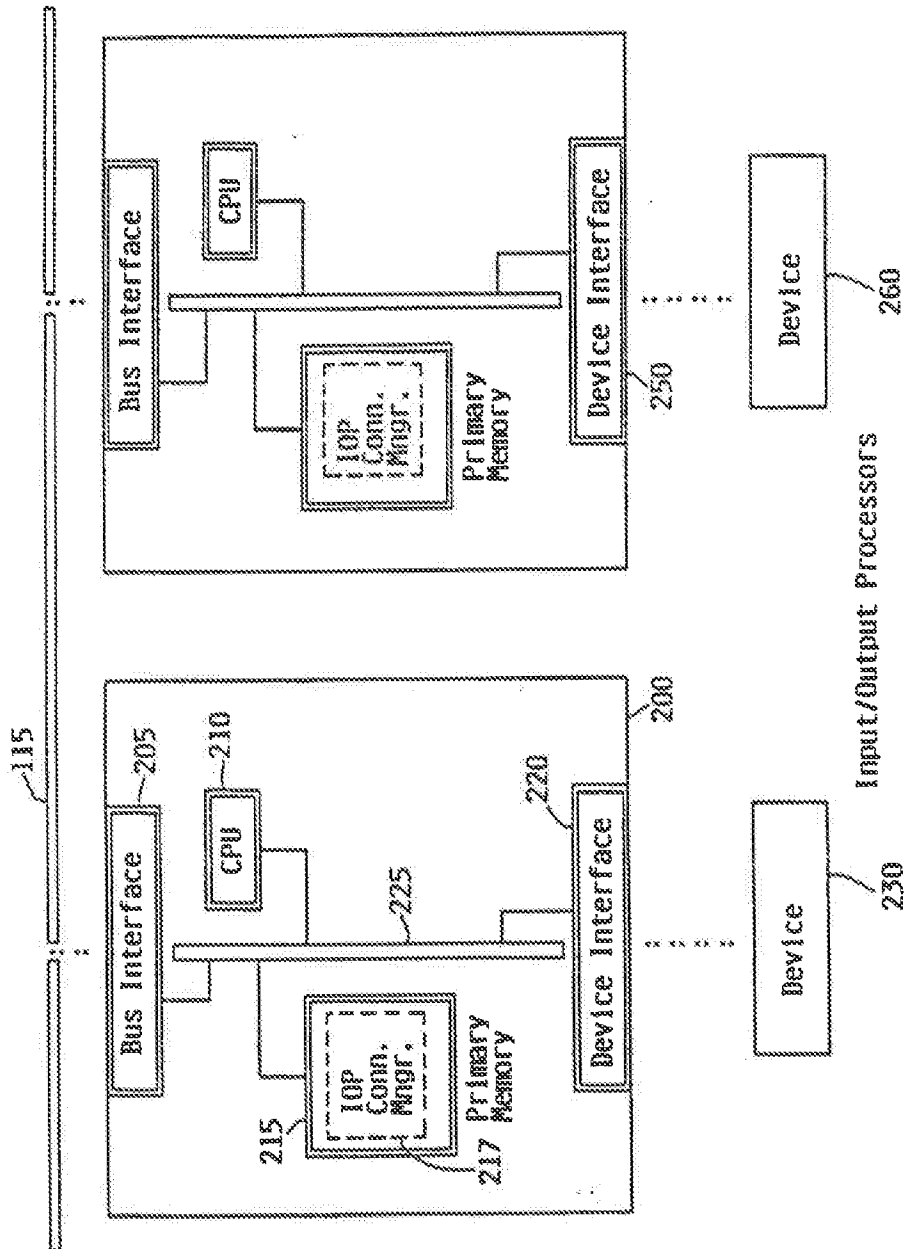
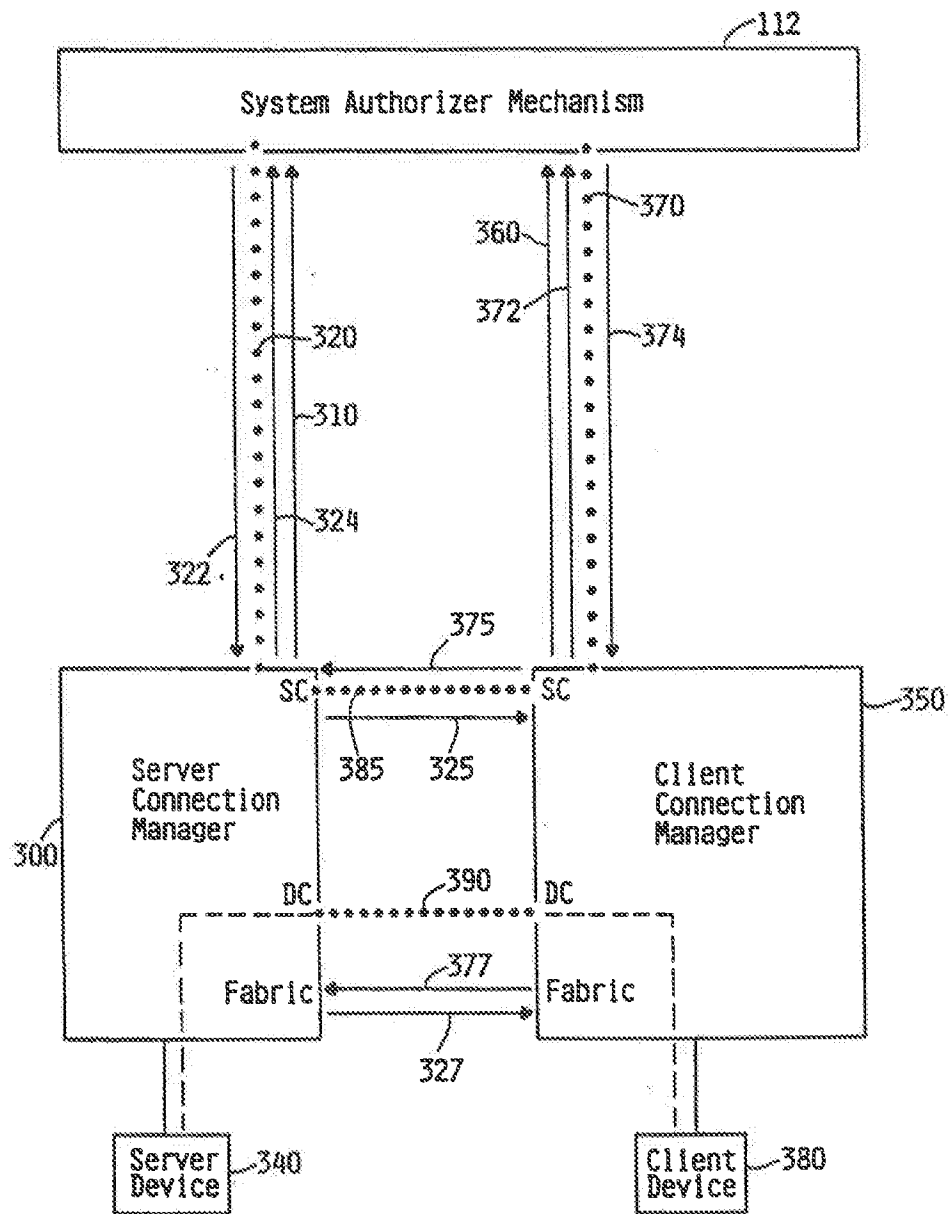


FIG. 2



*** = IPCF Logical Connection
 DC = Data Connection
 SC = Services Connection
 Fabric = Hardware Connection

FIG. 3

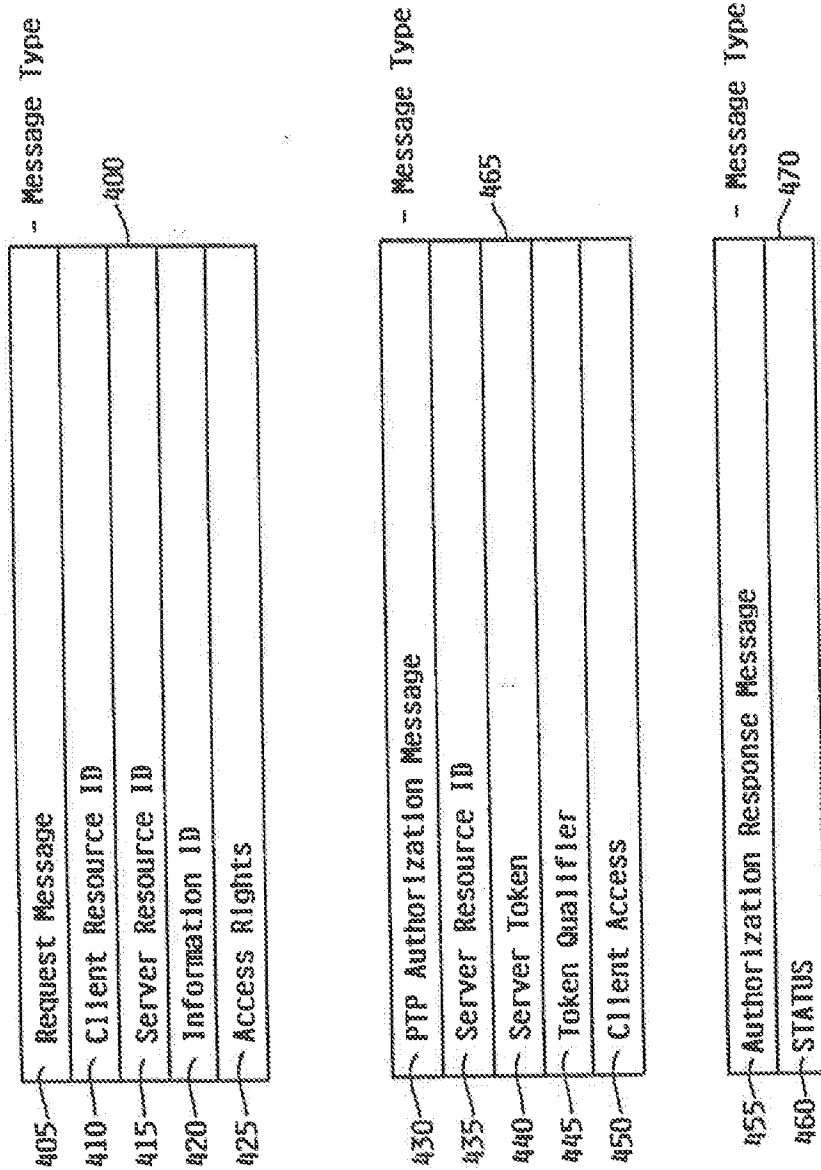


FIG. 4

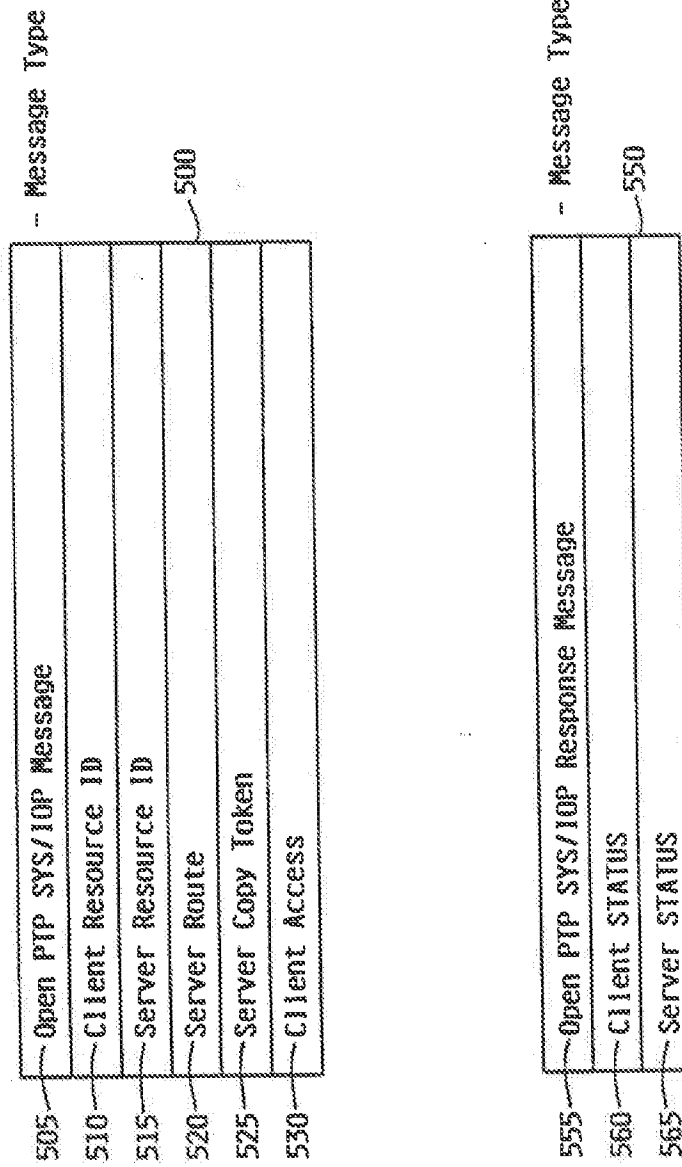


FIG. 5

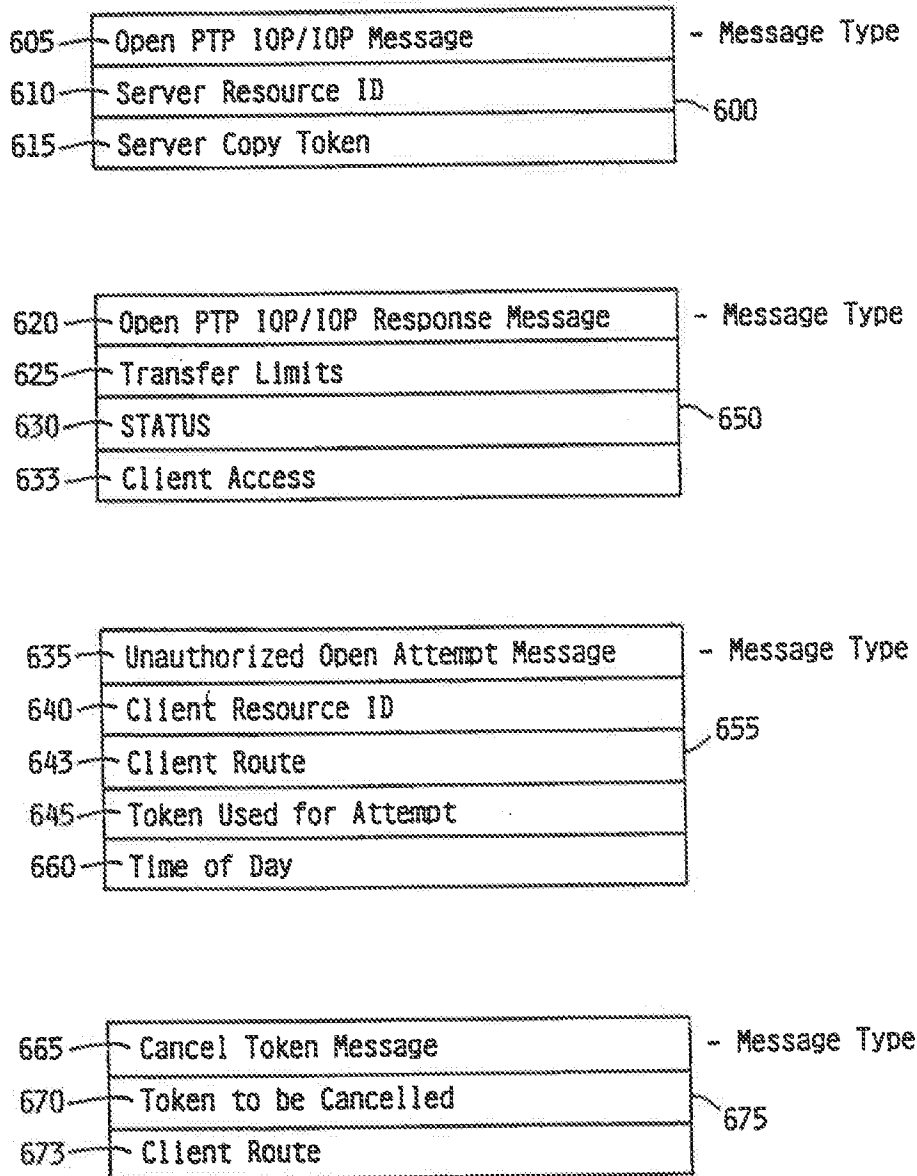


FIG. 6

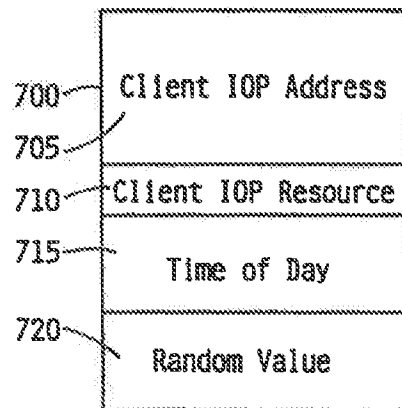
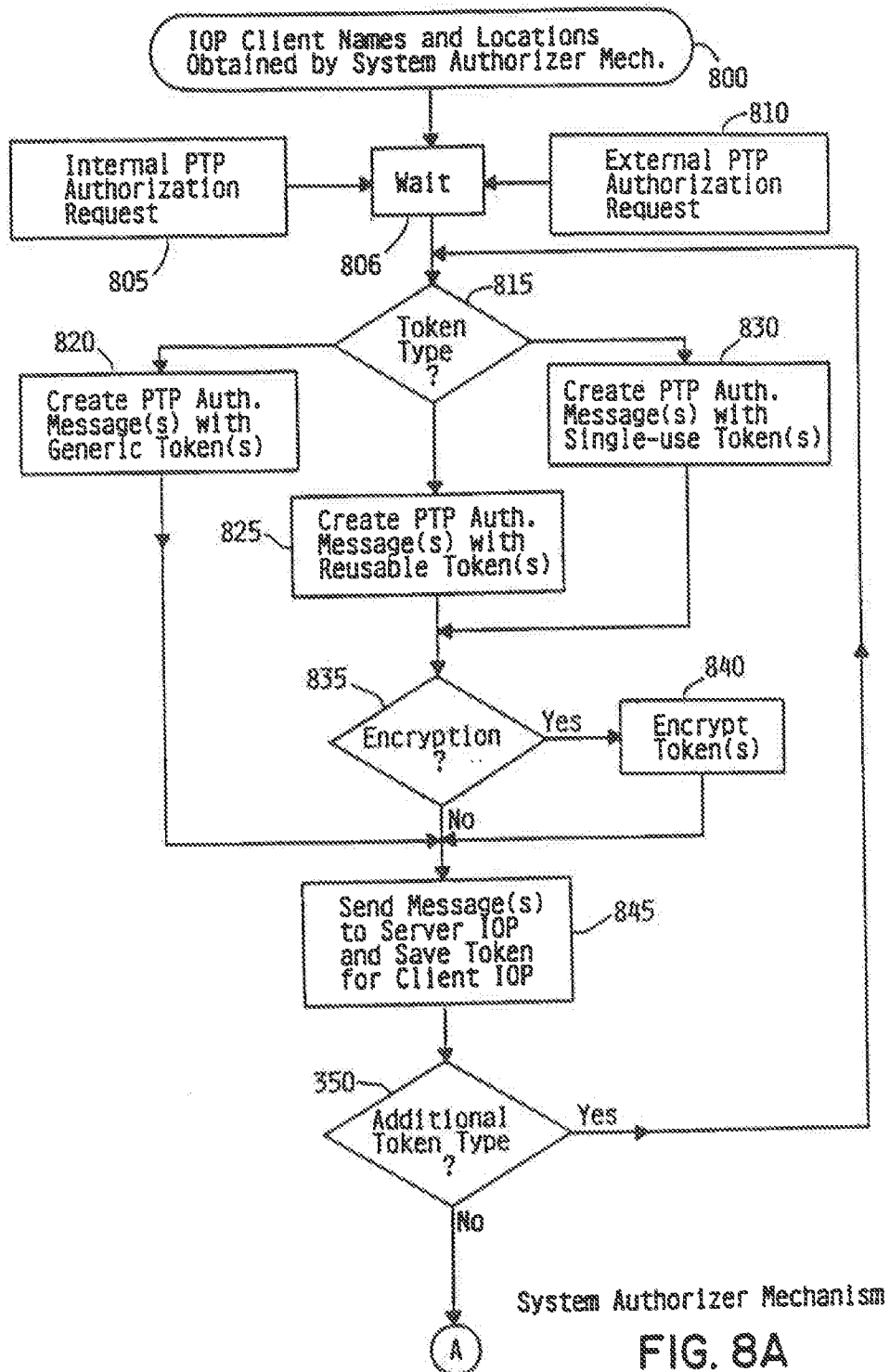
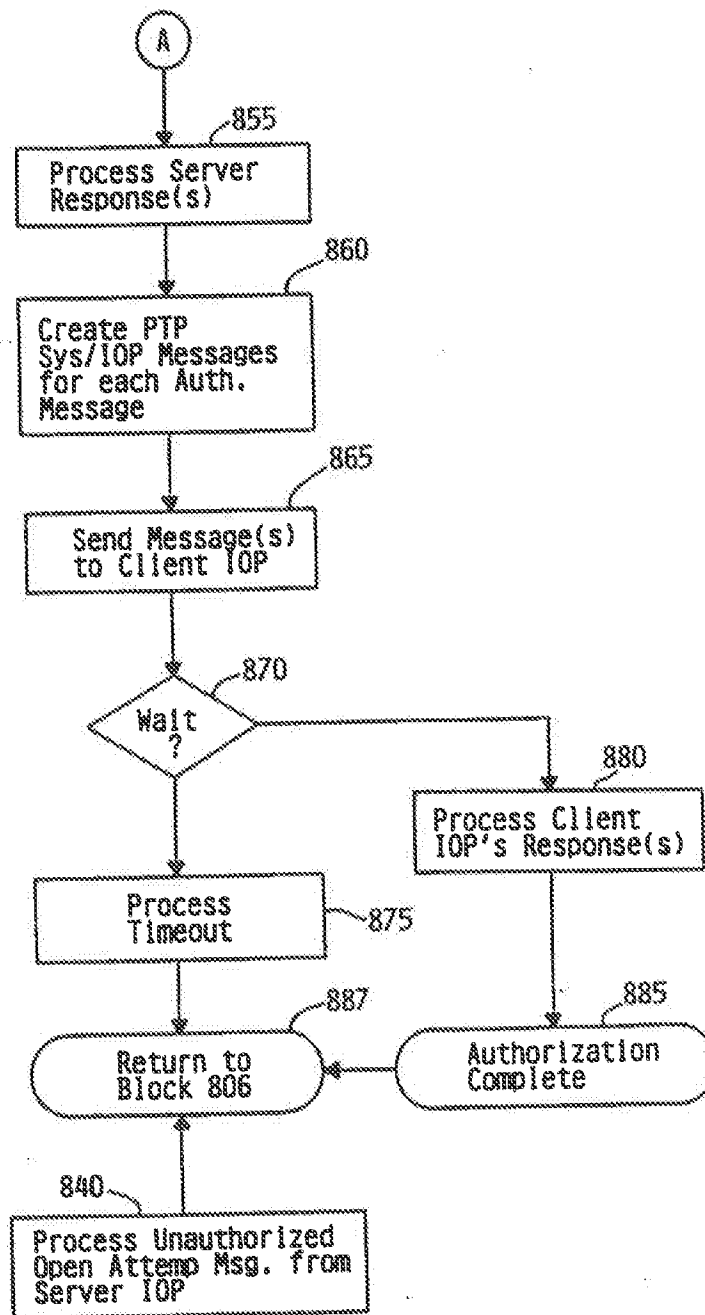


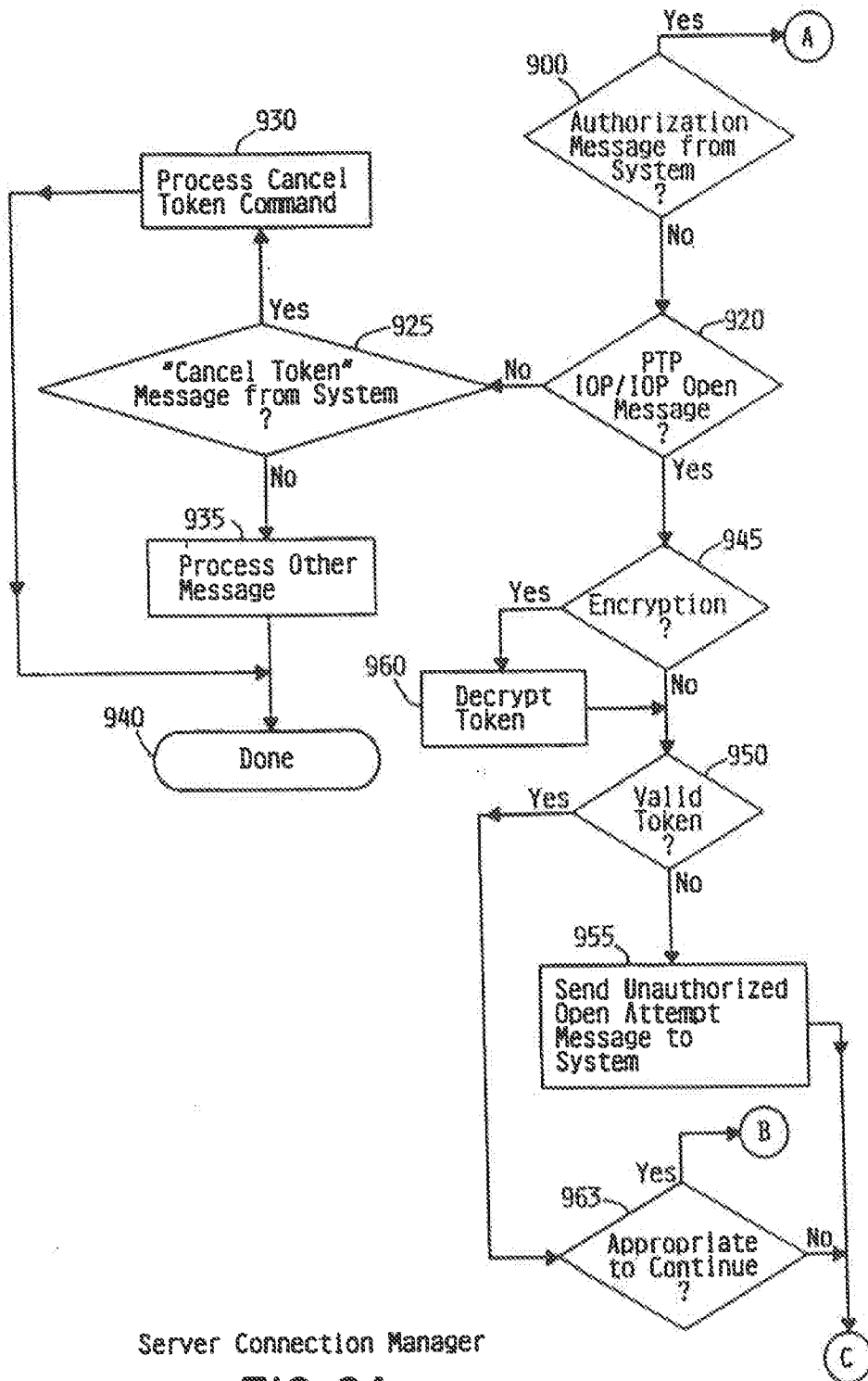
FIG. 7





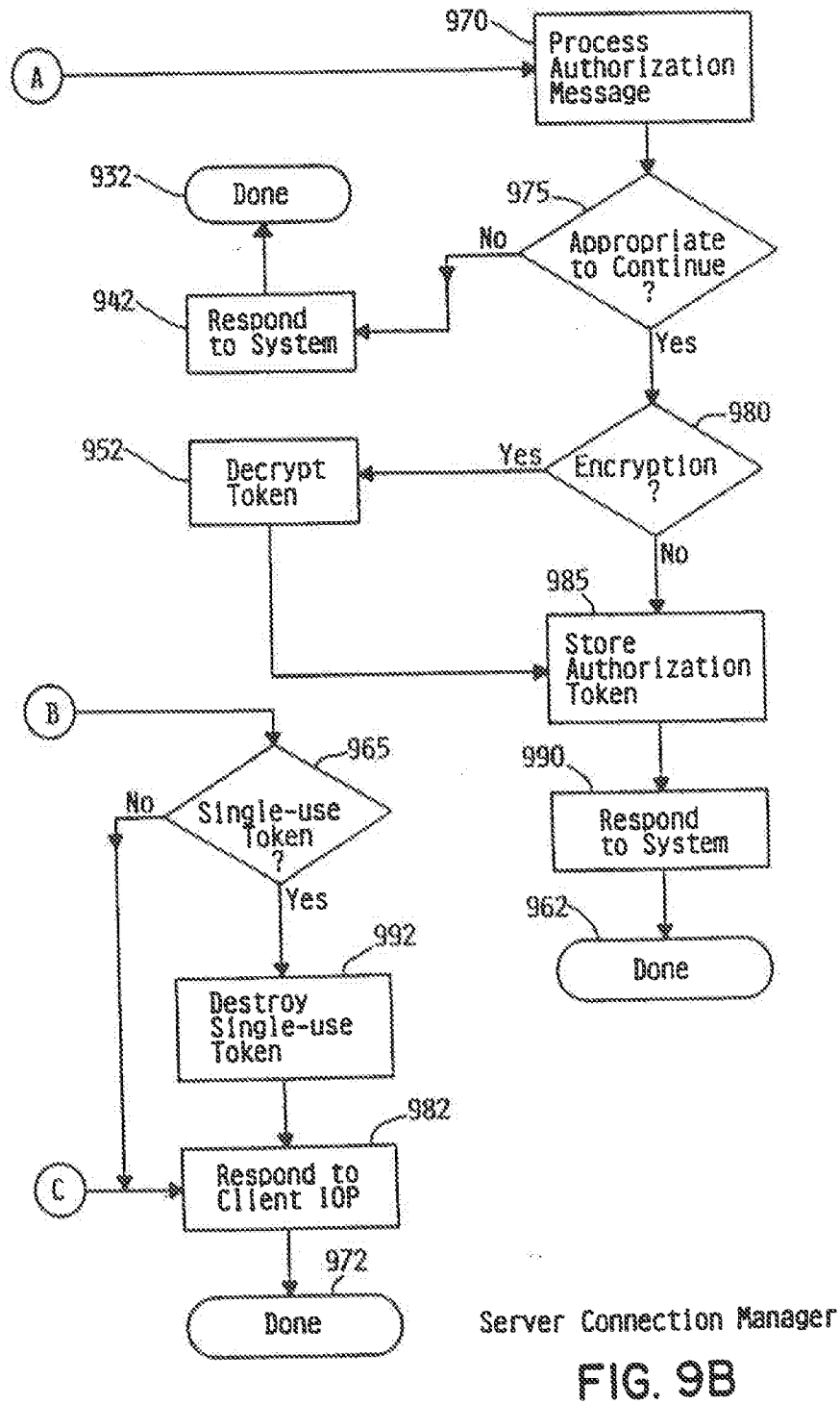
System Authorizer Mechanism

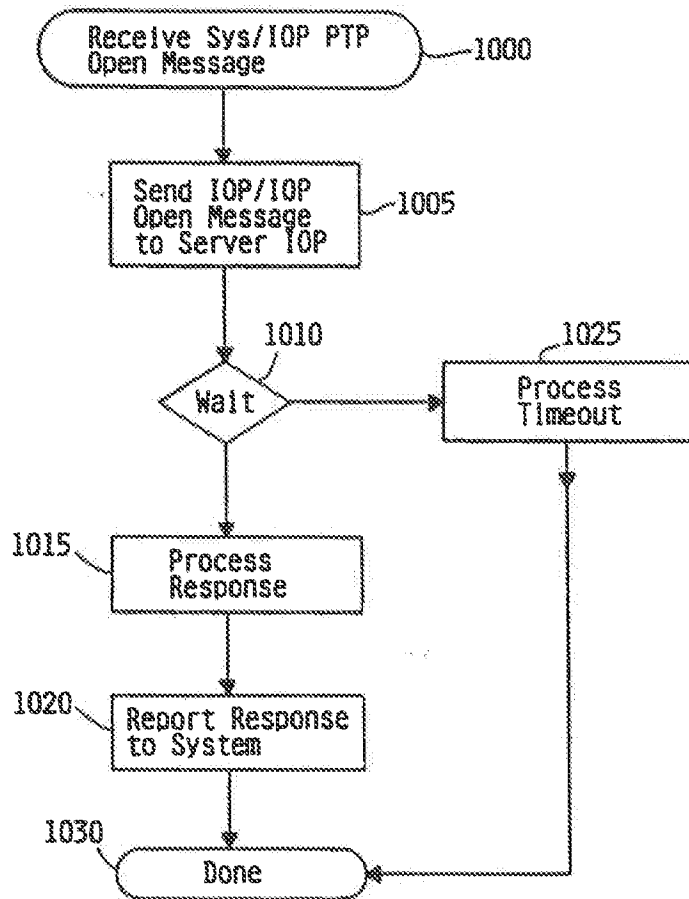
FIG. 8B



Server Connection Manager

FIG. 9A





Client Connection Manager

FIG. 10



European Patent
Office

EUROPEAN SEARCH REPORT

Application Number
EP 93 20 2581

DOCUMENTS CONSIDERED TO BE RELEVANT			
Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.CLS)
X	EP-A-0 281 224 (HEWLETT-PACKARD) * abstract; figure 1 * * page 4, line 1 - page 6, line 2 * * page 8, line 44 - page 10, line 45 * * page 17, line 7 - line 29 * * claims 1-8 * ----	1-16	G06F1/00 G06F12/14
D,A	US-A-4 649 473 (HAMMER ET AL) * the whole document * ----	1,3,5,7, 10,12, 13,15	
A	EP-A-0 115 348 (NEC) * abstract * -----	6,14	
			TECHNICAL FIELDS SEARCHED (Int.CLS)
			G06F
The present search report has been drawn up for all claims			
Place of search		Date of completion of the search	Examiner
THE HAGUE		22 December 1993	Powell, D
CATEGORY OF CITED DOCUMENTS			
X : particularly relevant if taken alone Y : particularly relevant if combined with another document of the same category A : technological background O : non-written disclosure P : intermediate document		T : theory or principles underlying the invention E : earlier patent document, but published on, or after the filing date D : document cited in the application L : document cited for other reasons * : member of the same patent family, corresponding document	

⑫ **EUROPEAN PATENT APPLICATION**

⑲ Application number: 90303877.8

⑤① Int. Cl. 8: G06F 1/00

⑳ Date of filing: 10.04.90

㉔ Priority: 15.05.89 US 352518

㉕ Date of publication of application:
 22.11.90 Bulletin 90/47

㉖ Designated Contracting States:
 DE FR GB IT

㉗ Applicant: International Business Machines
 Corporation
 Old Orchard Road
 Armonk, N.Y. 10504(US)

㉘ Inventor: Loucks, Larry Keith
 12801 Pickfair Drive
 Austin, Texas 78750(US)
 Inventor: Smith, Todd Allen
 1802 Apricot Glen
 Austin, TX 78746(US)

㉙ Representative: Bailey, Geoffrey Alan
 IBM United Kingdom Limited Intellectual
 Property Department Hursley Park
 Winchester Hampshire SO21 2JN(GB)

④ A flexible interface to authentication services in a distributed data processing system.

⑥ In a distributed data processing system, the authentication of a process at one node for the use of a service at another node is performed in a facility that is separate from the requester and service process. The separate facility is also replaceable, thereby allowing different authentication policies to be implemented within the distributed data processing system. The requesting process and the service process merely pass the authentication information between themselves without attempting to interpret the work of the separate authentication facility. In addition to authenticating the requester to the service, the service is also authenticated to the requester.

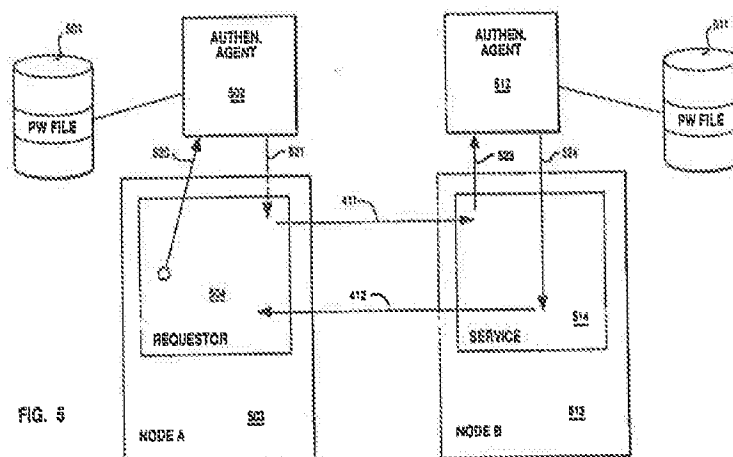


FIG. 5

A FLEXIBLE INTERFACE TO AUTHENTICATION SERVICES IN A DISTRIBUTED DATA PROCESSING SYSTEM

This invention relates to a flexible interface to authentication sources in a distributed data processing system including a plurality of data processing systems connected by a communications link, and to the authentication of a process at one of the data processing systems for the use of a service at another one of the data processing systems in a distributed networking environment.

5 A portion of the disclosure of this patent document contains material which is subject to copyright protection. The copyright owner has no objection to the facsimile reproduction by anyone of the patent document or the patent disclosure, as it appears in the Patent and Trademark Office patent file or records, but otherwise reserves all copyright rights whatsoever.

10 As shown in Fig. 1, a distributed networking environment 1 consists of two or more nodes A, B, C, connected through a communication link or a network 3. The network 3 can be either a local area network (LAN), or a wide area network (WAN).

At any of the nodes A, B, C, there may be a processing system 10A, 10B, 10C, such as a workstation. Each of these processing systems 10A, 10B, 10C, may be a single user system or a multi-user system with the ability to use the network 3 to access files located at a remote node. For example, the processing
15 system 10A at local node A, is able to access the files 5B, 5C at the remote nodes B, C, respectively.

Within this document, the term "server" will be used to indicate the processing system where the file is permanently stored, and the term "client" will be used to mean any other processing system having processes accessing the file. It is to be understood, however, that the term "server" does not mean a dedicated server as that term is used in some local area network systems. The distributed services system
20 in which the invention is implemented is truly a distributed system supporting a wide variety of applications running at different nodes in the system which may access files located anywhere in the system.

As mentioned, the arrangement to be described hereinafter is directed to a distributed data processing system in a communication network. In this environment, each processor at a node in the network potentially may access all the files in the network no matter at which nodes the files may reside.

25 Other approaches to supporting a distributed data processing system are known. For example, IBM's Distributed Services for the AIX operating system is disclosed in S.N. 014,897 "A System and Method for Accessing Remote Files in a Distributed Networking Environment", filed February 13, 1987 in the name of Johnson et al. In addition, Sun Microsystems has released a Network File System (NFS) and Bell Laboratories has developed a Remote File System (RFS). The Sun Microsystems NFS has been described
30 in a series of publications including S.R. Kleiman, "Vnodes: An Architecture for Multiple File System Types in Sun UNIX", Conference Proceedings, USENIX 1986 Summer Technical Conference and Exhibition, pp. 238 to 247; Russel Sandberg et al., "Design and Implementation of the Sun Network Filesystem", Conference Proceedings, Unix 1985, pp. 119 to 130; Dan Walsh et al., "Overview of the Sun Network File System", pp. 117 to 124; JoMei Chang, "Status Monitor Provides Network Locking Service for NFS", JoMei
35 Chang, "SunNet", pp. 71 to 75; and Bradley Taylor, "Secure Networking in the Sun Environment", pp. 28 to 36. The AT&T RFS has also been described in a series of publications including Andrew P. Rifkin et al., "RFS Architectural Overview", USENIX Conference Proceedings, Atlanta, Georgia (June 1986), pp. 1 to 12; Richard Hamilton et al., "An Administrator's View of Remote File Sharing", pp. 1 to 9; Tom Houghton et al., "File Systems Switch", pp. 1 to 2; and David J. Olander et al., "A Framework for Networking in System V",
40 pp. 1 to 8.

One feature of the distributed services system in which the disclosed arrangement is implemented which distinguishes it from the Sun Microsystems NFS, for example, is that Sun's approach was to design what is essentially a stateless server. This means that the server does not store any information about client nodes, including such information as which client nodes have a server file open or whether client processes
45 have a file open in read__only or read__write modes. Such an implementation simplifies the design of the server because the server does not have to deal with error recovery situations which may arise when a client fails or goes off-line without properly informing the server that it is releasing its claim on server resources.

In contrast an entirely different approach was taken in the design of the distributed services system in
50 which the disclosed arrangement is implemented which might be characterised as a "stateful implementation". A "stateful" server, such as that described here, does keep information about who is using its files and how the files are being used. This requires that the server have some way to detect the loss of contact with a client so that accumulated state information about that client can be discarded. The cache management strategies described here cannot be implemented unless the server keeps such state

information.

The problems encountered in accessing remote nodes can be better understood by first examining how a stand-alone system accesses files. In a stand alone system, such as 10 as shown in Fig. 2, a local buffer 12 in the operating system 11 is used to buffer the data transferred between the permanent storage 2, such as a hard file or a disk in a workstation, and the user address space 14. The local buffer 12 in the operating system 11 is also referred to as a local cache or kernel buffer.

In the stand-alone system, the kernel buffer 12 is divided into blocks 15 which are identified by device number, and logical block number within the device. When a read system call 16 is issued, it is issued with a file descriptor of the file 5 for a byte range within the file 5, as shown in step 101, Fig. 3. The operating system 11 takes this information and converts it to device number, and logical block numbers in the device, step 102, Fig. 3. If the block is in the cache, step 103, the data is obtained directly from the cache, step 105. In the case where the cache doesn't hold the sought for block at step 103, the data is read into the cache in step 104 before proceeding with step 105 where the data is obtained from the cache.

Any data read from the disk 2 is kept in the cache block 15 until the cache block 15 is needed for some other purpose. Consequently, any successive read requests from an application 4 that is running on the processing system 10 for the same data previously read is accessed from the cache 12 and not the disk 2. Reading from the cache is far less time consuming than reading from the disk.

Similarly, data written from the application 4 is not saved immediately on the disk 2, but is written to the cache 12. This saves disk accesses if another write operation is issued to the same block. Modified data blocks in the cache 12 are saved on the disk 2 periodically.

Use of a cache in a stand-alone system that utilises an AIX operating system improves the overall performance of the system since disk accessing is eliminated for successive reads and writes. Overall performance is enhanced because accessing permanent storage is slower and more expensive than accessing a cache.

In a distributed environment, as shown in Fig. 1, there are two ways the processing system 10C in local node C could read the file 5A from node A. In one way, the processing system 10C could copy the whole file 5A, and then read it as if it were a local file 5C residing at node C. Reading a file in this way creates a problem if another processing system 10A at another node A modifies the file 5A after the file 5A has been copied at node C as file 5C. The processing system 10C would not have access to these latest modifications to the file 5A.

Another way for processing system 10C to access a file 5A at node A is to read one block, e.g. N1, at a time as the processing system at node C requires it. A problem with this method is that every read has to go across the network communication link 3 to the node A where the file resides. Sending the data for every successive read is time consuming.

Accessing files across a network presents two competing problems as illustrated above. One problem involves the time required to transmit data across the network for successive reads and writes. On the other hand, if the file data is stored in the node to reduce network traffic, the file integrity may be lost. For example, if one of the several nodes is also writing to the file, the other nodes accessing the file may not be accessing the latest updated data that has just been written. As such, the file integrity is lost since a node may be accessing incorrect and outdated files.

In a stand-alone data processing system, file access control is often provided in order to protect sensitive information that users do not want to share with each other. A problem confronted with distributed data processing systems is how to distribute this same model of control and provide secure access to a user's information remotely while keeping other remote users from inadvertently or maliciously accessing or manipulating data belonging to another user.

Two problems that must be solved in order to provide a secure remote access for users are authentication and authorisation. Authentication is the process of identifying a user of a data processing system. Users typically accomplish authentication by presenting the user's name, or account number for the system, followed by a secret password which should only be known by that user. Presenting the secret password, which can be validated by the system, allows the system to authenticate the user to be who the user claims to be. Once authenticated, the system may then authorise this user to have access to resources managed by the data processing system. Therefore, authentication is the identification of a user, and authorisation is the granting of a privilege to a user to gain some kind of access to the system.

As mentioned above, authentication of local users is often accomplished through the use of a shared secret. This secret is typically a password which the user enters at a prompt. The system then compares this password to a recorded version of the password. If the system determines that the password is correct, the user is authenticated. Remote authentication is more difficult than that previously described.

A procedure for remote authentication is described in the following papers. "Kerberos: An Authentica-

tion Service For Open Network Systems", Steiner, Jennifer G.; Neuman, Clifford; Schiller, Jeffrey I.; pages 1-15, USENIX, Dallas, TX, Winter, 1988. "Project Athena Technical Plan, Section E.2.1, Kerberos Authentication and Authorisation System", Miller, S.P.; Neuman, B.C.; Schiller, J.I.; Saltzer, J.H.; pages 1-36, Massachusetts Institute of Technology, October 27, 1988. These above two references are herein incorporated by reference. This Kerberos based remote authentication authenticates users working at one node in a distributed data processing system to services running on the same node or other nodes in the distributed system. A distinctive property of the Kerberos protocol is that users can be authenticated with services running on nodes which share no secret with the user. If a simple password based authentication scheme were used, each user would have to share a secret with each machine in the entire distributed system. By using the Kerberos protocol, users need to share a secret with only one machine; the machine running the Kerberos authentication service.

Kerberos authentication works as follows. In order to be authenticated to a remote service, the user must present a specially constructed data structure, called a ticket, to the service that the user wishes to be authenticated to. This ticket is particular to the user and the service. That is, each service requires that these tickets are tickets intended for that service. Moreover, these tickets are specially constructed for an individual user who wants to be authenticated. These tickets are issued by the part of the Kerberos authentication server called the ticket granting service. Before using the service, say a remote print server, a user acquires a ticket for that print server. The user requests the Kerberos ticket granting service to issue a ticket for that user for the use of the print server. The Kerberos ticket granting service constructs the ticket, gives it to the user, and the user presents it to the print server. The print server examines the ticket and can determine that the sender was indeed the claimed user.

In detail, this Kerberos scheme is more complex in order to ensure that tickets can not be forged or stolen by another user. In addition, the messages for passing tickets between machines are designed such that the messages can not be recorded and replayed. The Kerberos scheme also ensures that the user can not trick the ticket granting service itself. This last step can be accomplished by requiring a ticket to use the ticket granting service. This master ticket is acquired by users before any other ticket can be issued for that user. Once a user has a master ticket, the user can present the master ticket to the ticket granting service and be issued tickets for other services in the distributed system.

Another distinctive feature of the Kerberos authentication scheme is that while the user must go to the authentication server to request tickets, the service to which these tickets are being presented does not need to communicate with the Kerberos authentication service during the user authentication.

The Kerberos protocol provides a sophisticated authentication scheme. However, such schemes are not appropriate for small networks where the overhead in administering a Kerberos server may not justify its use. In such cases, other authentication schemes are possible which may just simply involve the sharing of a secret between every user and every node in the distributed system. If the distributed system has only a few machines, such as three or so, it may be easier for each user to maintain a password on each machine and to authenticate that password periodically to ensure that the users are not compromised.

A third possible authentication scheme might be appropriate for networks that are larger than those that can be conveniently managed by users needing individual passwords on each machine yet are smaller than would justify a Kerberos authentication protocol. This third scheme might use a centralised authentication server which all of the nodes communicate with. A password might be presented to a remote service by a user, and the remote service checks with the central authentication server to determine whether the password is correct. This requires services to communicate with the authentication server instead of users. This is in contrast to the Kerberos scheme where services do not need to communicate with the authentication server during user authentication.

As illustrated above, there is a wide range of possible implementations of authentication servers that may be appropriate for distributed systems providing user authentication.

An operating system, such as the AIX operating system, which provides for distributed functions such as in Distributed Services of the AIX operating system, uses remote authentication to authenticate client machines to servers, servers to client machines, and users to server machines. However, it may be desirable to run an operating system having distributed functions in various sizes of networks having a range of nodes from one or two nodes to hundreds or thousands of nodes.

Consequently, an operating system providing distributed functions must run in the presence of various authentication schemes from the simplest most straight forward scheme to the most complex and sophisticated scheme.

An efficient way of implementing a distributed services function of an operating system is to modify the operating system kernel to support distributed service operations. This includes the communication between nodes and the management and synchronisation of the facilities being distributed. When a user operation

on one machine causes a request to be sent to a remote machine, that user must be authenticated to the remote machine. This activity causes programs to be executed at the remote machine. The distributed service function of the operating system must perform the authentication of the remote user, but to do so, it must use the network's authentication scheme, for which various schemes are possible and can operate
 5 very differently from one another. Additionally, this authentication may require communications with the remote authentication server at either the user side or at the remote machine side. Since it is impossible to anticipate all possible authentication schemes that the network may be using, it is desirable for a distributed service function of the operating system to have a flexible authentication protocol that allows it to use whatever available authentication scheme is running on the network.

10 For example, a distributed service of the operating system gets to a remote machine with a request from a user, but the remote machine may discover that it has never seen this user before. The remote machine then may require the user to authenticate itself to the remote machine. However, the distributed service function may not know how the authentication is to be performed. If the distributed service function determined how the authentication process is to be performed, this would limit the users of the distributed
 15 service function of an operating system to the one predetermined authentication scheme.

Furthermore, if the predetermined authentication scheme requires remote communications with the server, there is a variety of exceptions and failures which are difficult to provide for inside the kernel of the operating system at the point where the authentication process would need to be performed. If the communications to the authentication server breaks, and the authentication process is inside the kernel, all
 20 processing within the data processing system may come to a halt while the operating system kernel is waiting while trying to communicate with the remote authentication server.

To alleviate such shortcomings, the present invention provides a system having means for authenticating a requester, at a first node, of a service running at a second node, wherein the requester and the service are connected by a means of communication in a distributed data processing system, the system
 25 comprising: means for constructing authentication information by a facility, supporting an authentication policy, separate from the requester; and means for determining, at the second node, from the constructed authentication information, an authentication of the requester.

The present invention also provides a system having means for authenticating a requester, at a first node, of a service running at a second node, wherein the requester and the service are connected by a
 30 means of communication in a distributed data processing system, the system comprising: means for constructing authentication information and an authentication acknowledgement by a facility, supporting an authentication policy, separate from the requester; means for sending, by the requester, the authentication information to the service running at the second node; means for processing the sent authentication information at a second facility, supporting the authentication policy, at the second node separate from the
 35 service; means for acquiring, by the service, an outcome of the processing for determining a first authentication of the requester and a second authentication acknowledgement; means for receiving, by the requester, the second authentication acknowledgement; and means for comparing, by the requester, the first authentication acknowledgement and the second received authentication acknowledgement for determining a second authentication of the service.

40 The present invention also provides method for authenticating a requester, at a first node, of a service running at a second node, wherein the requester and the service are connected by a means of communication in a distributed data processing system, the method comprising: constructing authentication information by a facility, supporting an authentication policy, separate from the requester; and determining, at the second node, from the constructed authentication information an authentication of the requester.

45 The present invention also provides a method for authenticating a requester, at a first node, of a service running at a second node, wherein the requester and the service are connected by a means of communication in a distributed data processing system, the method comprising: constructing authentication information and an authentication acknowledgement by a facility, supporting an authentication policy, separate from the requester; sending, by the requester, the authentication information to the service running
 50 at the second node; processing the sent authentication information at a second facility, supporting the authentication policy, at the second node separate from the service; acquiring, by the service, an outcome of the processing for determining a first authentication of the requester and a second authentication acknowledgement; receiving, by the requester, the second authentication acknowledgement; and comparing, by the requester, the first authentication acknowledgement and the second received authentication
 55 acknowledgement for determining a second authentication of the service.

The present invention also provides a method for use on a first data processing system having means for requesting, by a process at the first data processing system, a service at a second data processing system connected to the first data processing system through a means of communication, the method

comprising: sending a message to a replaceable facility, supporting an authentication policy, separate from the requesting process, to initiate authentication by constructing authentication information; and sending, unaware of the contents of the constructed authentication information, the constructed authentication information, with a request to use the service, to the service for becoming authenticated to use the service.

5 The present invention also provided a method for use on a second data processing system having means for receiving a request, from a process at the first data processing system, for a service, the second data processing system connected to the first data processing system through a means of communication, the method comprising: sending authentication information, received from the process, to a replaceable facility, supporting an authentication policy, separate from the service, for an interpretation of the authentication information and a construction of a plurality of authentication credentials; receiving the constructed
10 credentials from the separate facility; performing an operation on the request based on the received credentials; and returning to the requesting process a result of the operation and the authentication acknowledgement received from the separate facility.

The present invention also provides a method for use with at least one data processing system, the
15 method comprising: receiving a message from a process to initiate authentication of the process in response to a request by the requesting process to use a service of a different process; constructing authentication information and an authentication acknowledgement from requester information and service information found in the received message; sending the constructed authentication information and the authentication acknowledgement to the requesting process; receiving the constructed authentication in-
20 formation from the service; constructing a plurality of credentials from the received authentication information for the service and a second authentication acknowledgement; and sending the constructed credentials and the authentication acknowledgement to the service.

The system and method disclosed hereinafter defines an interface between an operating system providing distributed service functions and a user program providing an authentication scheme. This
25 interface is well defined and highly structured such that the kernel of the operating system does not change at all depending upon the authentication services in the network that are being utilised. A program providing an authentication scheme can be interchangeable with other authentication programs whenever the authentication scheme changes in the network. In addition, utilising a user program at the remote machine to perform the authentication allows the user program to be killed, restarted, and scheduled as a regular
30 program without affecting the performance of the underlying operating system. The complexity of authentication lies in the program and not in the kernel of the operating system.

An authentication daemon program is used at both the user initiating node and the receiving service node. A set of message flows allows a distributed service function within the operating system to use the results of these authentication daemons in a way that is transparent to the distributed services function. The
35 distributed services function merely passes the information back and forth without attempting to interpret the work of the authentication daemon. Accordingly, different authentication daemon programs using different authentication schemes can be used interchangeably within the network without affecting or changing the underlying distributed service function of the operating system. Likewise, the same distributed service function can be used within various networks having different authentication schemes in the
40 authentication daemon used in each network.

More specifically, a request sent to a remote service that requires authentication includes an object called the authentication information object. This authentication information object and an associated authentication acknowledgement value are constructed, at the requester's node, by the authentication daemon from information about the requester. The contents of these authentication items and the means for
45 their construction are preferably unknown outside of the authentication daemon itself. The authentication acknowledgement value is retained and the authentication information object is included in the message used for the request. The service, before performing the request, extracts the authentication information object from the request and passes it to a second authentication daemon running at the service's node. This second authentication daemon uses the authentication information object to authenticate the requester
50 according to the authentication policy supported by the daemons. The second authentication daemon also returns a second authentication acknowledgement value that is returned to the requester in the reply to the request. This second authentication acknowledgement is compared with the first authentication acknowledgement previously retained by the requester to ensure that the identity of the remote service is that of the intended service.

55 The present invention will be described further by way of example with reference to an embodiment thereof and a contrasting prior art arrangement, both as illustrated in the accompanying drawings in which:

Fig. 1 is a block diagram of a distributed data processing system known in the art;

Fig. 2 is a block diagram showing a stand-alone data processing system known in the art for

accessing a file through system calls;

Fig. 3 is a flow diagram of the data processing system of Fig. 2 accessing a file through a system call;

Fig. 4A is a request__for__service message which is used by a process running on a client machine in order to request that a remote service be performed;

Fig. 4B illustrates the messages that flow between the authentication agent and the requester and between the authentication agent and the service;

Fig. 5 shows a client data processing system and a server data processing system in a distributed data processing system having a separate authentication agent for performing authentication; and

Fig. 6 is a flow showing the operations of the requester, the authentication agent, and the service.

With reference to Figure 4A, the internode message request__for__service 410 used herein is described. The request__for__service message 410 is used by a process running on a client machine in order to request that a remote service be performed. The request 411 has an opcode 413 indicating the specific operation requested. The request 411 also has an operation field 420 used to indicate the desired operation to be performed by the server. The authentication info field 416 in the request is used to pass enough information to the remote machine to authenticate the process performing the request. The remote machine responds with the reply 412. The opcode field 414 indicates that this is the reply for the particular kind of request. The return code (rc) 417 in the reply is used to indicate the success or failure of the remote machines attempt to execute the request. An acknowledgement is returned in the ack field 419. The ack is used to verify that correct identification between the requesting process and the remote machine has occurred.

Fig. 4B shows the messages that flow between the authentication agent and the requester and between the authentication agent and the service.

The requester to authentication agent message 520 contains information describing the requester 531 and information describing the service 532 that the request will be sent to. The authentication agent to requester message 521 contains an authentication information object 416 and an authentication acknowledgement value 534. The service to authentication agent message 523 contains only the authentication info object 416. The authentication agent to service message 524 contains another authentication acknowledgement value 419 and a set of credentials 536 that are used by the service to authenticate the requester.

Referring to Fig. 5, a machine 503 contains a requester 504 that makes use of an authentication agent 502 through messages 520, 521. The authentication agent 502 refers to data stored on disk 501. A second machine 513 contains a service 514 that makes use of an authentication agent 512 through messages 523, 524. The requester 504 communicates with the service 514 via the request__for__service request 411 and its reply 412.

In the preferred embodiment, a first machine 503 is communicating with a second machine 513 over a network. Rather than performing the authentication operation within the requester process 504 and the service process 514, which may be running in an operating system of the machines, the authentication operation is performed in the authentication agent programs 502, 512 at both of the nodes. These authentication agents may be user level programs as used in systems running any type of operating system or daemons as used in systems executing the AIX operating system or other operating systems based on the UNIX operating system.

The following description refers to Fig. 4A, Fig. 4B, Fig. 5, and Fig. 6, concurrently. Before a process at a first machine begins to send a request 411, step 601, to use the services of a second machine, an authentication procedure must first be performed. The requesting process 504 sends a message 520 to the first authentication agent 502 at the first node in order to initiate authentication, step 602. This message contains information 531 describing the process making the request and information 532 identifying the requested service.

The first authentication agent 502 uses the contents of the message 520 to construct a reply 521, step 603, returned to the requesting process, step 604. This reply 521 contains authentication information 416 and an authentication ack 534. The way in which the authentication agent uses the contents of message 520 depends upon the particular authentication policy being supported; but the way that the requesting process uses the reply 521 is independent of the policy supported by the authentication agent. The requesting process does not interpret either the authentication information 416 or the authentication ack 534. The only operations that the requesting process needs to perform with these elements are the transmission of the authentication information to the remote service in a request, steps 605, 606 and a bitwise comparison for equality between the authentication ack 534 received and retained, step 606, from the local authentication agent 502, and the authentication ack 419 in reply 412 received from the remote service.

In addition, the service receiving the request 411 does not need to interpret the information contained in the authentication information field 416. The service, like the requester, trusts the authentication information in the same manner independent of the authentication policy that it supports. The service always passes the authentication information to the authentication agent 512, step 607, where interpretation of this information is performed, step 608. The agent will find different contents in the authentication information message 523 depending upon the particular authentication policy being supported by the authentication agents 502 and 512. In the message 524 sent from the agent 512 to the service 514, step 609, the agent places a set of credentials 536 that describe the remote requester in a manner that is meaningful to the service. Additionally, the agent places an authentication ack 419 in this message that does not need to be interpreted by the service. Like the authentication information, the authentication ack 419 is treated in the same manner by the service for all authentication policies supported by the authentication agents. The only operation that the service performs on the authentication ack 419 is returning it to the requester in reply 412. The service makes a determination, step 610, based on the credentials 536 on the authentication and authorisation of the requester's permission to request an operation 420 of the service, conditionally performing the requested operation, step 611. The results of this determination and operation are returned in a return code 417 to the requester in a reply message 412 along with the authentication ack 419, step 612.

The requester receives the reply 412 and extracts the authentication ack 419 and compares it to the authentication ack 534 previously received from the local authentication agent 502, step 613. If the two acks are bitwise equal, the requester is assured of the remote service's identity to the limit of the ability of the authentication protocol supported by the agents. Upon verifying the identity of the service, the requester examines the return code 417 to determine the outcome of the original request, step 614, completing the request for service, step 615.

The following programming design language code illustrates the processing at the authentication agent.

```

/* authentication agent */
LOOP FOREVER
5      await message;
      IF request is a requester to agent message THEN
          use requester information found in message
          along with the service information
10         found in the message to construct both
          authentication information and
          an authentication acknowledgement;
15         send message reply containing
          authentication information and
          authentication ack
          back to requester;
20     ELSE /* request is a service to agent message */
          use the authentication info to construct a
          set of credentials and
25         an authentication ack;
          send message reply containing
          the set of credentials and
30         the authentication ack
          back to service;
      ENDIF;
35  ENDLOOP;

```

Copyright IBM Corporations 1989

40 The following programming design language code
illustrates the processing at the requester.

```

/* requester */
45
/* about to make a request of a remote service */
construct a message containing a description of the
50 process making the request and a description of
the remote service;

```

55

```

send this message to authentication agent;
await reply from authentication agent;
save the authentication ack returned in reply from
5      agent;
construct a request for remote service, include
      authentication information returned in reply
10     from the authentication agent;
send request to remote service;
await reply from the service;
IF authentication ack in reply from service
15     = saved authentication ack THEN
      /* remote service authenticated */
      examine the result of the remote operation;
20     ELSE
      /* remote service not authenticated */
      /* ignore the returned return code */
25     ENDIF;

```

Copyright IBM Corporation 1989

The following programming design language code illustrates the processing at the service.

30

35

40

45

50

55

```

/* service */

LOOP FOREVER;
5      await request from a remote requester;
      extract the authentication information from the
      request;
10     send authentication information to the
      authentication agent;
      await reply from agent;
15     extract credentials for remote requester from the
      reply;
      extract authentication ack from the reply and
      save it;
20     IF credentials indicate that the requester has
      permission to have the server perform the
      operation requested in the request from the
25     requester THEN
      perform the operation;
      return code := the results of the operation;
      ELSE
30     return code := value indicating permission
      failure;
      ENDIF;
35     construct a reply containing the return code and
      the saved authentication ack;
      send reply back to the server;
40     ENDLOOP;

```

Copyright IBM Corporation 1989

45 Note, that the design suggested above employs messages to communicate between the service and the authentication agent and between the requester and the authentication agent. These messages are shown in Fig. 4B. This choice of communication interface is intended to allow multiple processes, either requesters or services or combinations of the two, running on the same node to use a single agent. In the preferred embodiment using the AIX operating system the interprocess communication facilities called message queues provide this type of interface. These message queue facilities are described in the "AIX Operating System Technical Reference", second edition, September, 1986, order number SV21-8009, part number 74X9990, hereby incorporated by reference, and more specifically pages 2-71 to 2-85. This allows multiple processes to share the authentication daemon process. By using a well defined interface based on messages, the preferred embodiment allows the daemon process to be replaced without necessitating any changes in its clients, i.e., the requesters and the services.

55 For example, if Kerberos based authentication is being performed, the agent will acquire a Kerberos ticket for the requester to use the remote service. This may involve searching id to name tables stored in the password file on disk 501 or ticket caches stored on disk 501 or memory. It may further involve

communication with a remote Kerberos server using the Kerberos protocols. If Kerberos is used, the authentication info 416 contains all of the information that is needed by a service to authenticate a remote requester using Kerberos.

To illustrate how the preferred embodiment can be used to support the kerberos protocol, the steps performed by the authentication agent are further described. Message 520 to the authentication agent is used by the agent to determine the requesting process's associated user id. In the preferred embodiment, this id is contained in the field 531 describing the requester and is a small integer used to identify the user on whose behalf the request is running. The authentication agent uses this id to locate the Kerberos tickets owned by this user. In the preferred embodiment, the agent will find these tickets in a file located on the disk 501 under the name /tmp/tkt(uid) where (uid) is the actual user id. In this file, a ticket for the requested service described by field 532 may be found. If such a ticket is not found, a new ticket for the requested service is acquired by the agent. The agent acquires a new ticket by sending a ticket request to the Kerberos ticket granting service. This ticket request is constructed according to the requirements of the Kerberos protocol as described in "Kerberos Authentication and Authorisation System", Miller, S.P. et al. Basically, the agent constructs an encrypted authenticator containing a timestamp and sends it, along with a ticket for use of the ticket granting service, to the ticket granting service in its requests for a ticket to the desired service.

In response to the ticket request, the authentication agent will receive from the ticket granting service a ticket for the desired service and a session key for use with this service. The agent will also construct an authenticator encrypted with the session key and combine this with the ticket just received. The agent places this in the authentication info field 416 of the reply 521 that is returned to the requester. Additionally, the agent will construct an authentication ack from the value of the timestamp placed in the encrypted authenticator. It does this by adding one to the timestamp and encrypting it with the session key. This authentication ack is placed in field 534 of the reply.

The requester, upon receiving the reply 521, does not need to be aware that the authentication field and the authentication ack are constructed in order to take advantage of the Kerberos authentication protocols. Instead, the requester treats these as abstract values, handling them in the same way independent of the way in which the authentication agents are performing authentication. The authentication info field is sent to the remote service in message 411 where it is passed in message 523 to the authentication agent running at the remote node. The remote authentication agent obtains, from the ticket, verification of the remote requester's identity and the session key that will be used with this remote requester. This information is encrypted in the ticket in a manner which makes tickets unforgeable.

Additionally, the remote agent checks the authenticator sent with the ticket, decrypting it with the session key, to find the timestamp. The timestamp is examined to make sure that this request is not a replay of a previous request. The timestamp is also used to construct an authentication ack in the same manner as was done by the first authentication agent. The authentication ack is returned to the service in field 419 along with a description of the requester's identity in field 536 of message 524. The ack constructed at the service authentication agent is then returned in message 412 to the requester where it is compared to the authentication ack constructed at the requester's node. This completes a Kerberos based authentication scheme using the preferred embodiment.

While performing the above described request, the agent communicates with the Kerberos ticket granting service. This may be running on a remote node and hence require network communication. This is not a problem for the agent since it is a regular scheduled process which can be put to sleep while awaiting a reply from the Kerberos ticket granting service without adversely impacting the performance of other processes on the system where the agent is running. If the requester had attempted to acquire the tickets directly without going through an authentication agent, the requester might have to sleep awaiting an I/O request. This could impact system performance adversely if the requester was running under kernel state in some operating systems. Furthermore, some operating systems cannot initiate I/O such as this while in the middle of processing a previous I/O request for a process. This can occur if a process attempts to perform I/O on a remote file. While in the middle of an I/O request for a remote file, it may be discovered that authentication operations need to be performed that involve I/O such as communicating with the Kerberos ticket granting service, causing problems in systems where a separate authentication agent is not used. In this preferred embodiment, authentication operations can be performed by the separate agent while a requesting process is in a state where it would not be able to perform the I/O necessary for the authentication at that time.

Likewise, a different authentication policy can be used in conjunction with this preferred embodiment. When the authentication agent receives message 520 it obtains the user id from field 531. It should be noted that in the preferred embodiment all information that might be used by an authentication policy is

passed in field 531 so that different implementations of a policy or different policies running in the agent will find all information needed in this field. The user id is used to search the password file on disk 501 for a password that this user has prearranged to use with the remote service identified by field 532. This password and an associated reply password are obtained by this lookup operation. The password is placed in field 416, the authentication info field, and the reply password is placed in field 534, the authentication
 5 ack field, of the message 521. The requester sends the authentication info field 416 to the service where it is passed to the remote agent in message 523. The remote agent uses the password to search a file stored on disk 511 to locate a description of the identity of the requester. If found, this identity information is placed in field 536 along with a reply password found in the same file and placed in field 419, the
 10 authentication ack field of message 524. The service returns the authentication ack value to the requester where it, the reply password found at the service node, is compared with the authentication ack obtained from the requester authentication agent, the reply password found in the local file. If they are the same, successful mutual authentication has occurred.

Another possible authentication policy might be implemented with a centralised authentication system.
 15 Like the scheme just described, the authentication info field is a password passed from the requester to the service and checked in the service authentication agent. The authentication ack is a reply password passed to the requester from both the requester authentication agent and the service, which obtains it from the service authentication agent. Instead of finding these passwords in files on disks 501, 511, these passwords are obtained from a centralised authentication system by the agent.

20 Finally, the agents may be in direct communication with each other. This allows authentication policies that work outside of the network used for request for service operations to be supported. For example, a physically secured communication channel between the agents could be used to dynamically determine appropriate authentication info values and authentication ack values. Requesters and services can communicate over lower cost or more available communication channels while achieving secure authentication
 25 through the use of the preferred embodiment where the agents communicate over a single secure channel.

It should be noted that the process acting as the authentication agent in a node can act in both roles, as the requester authentication agent and the service authentication agent because both services and requesters may be running in the same machine.

Simply by disconnecting the authentication daemons, and replacing them with another authentication
 30 daemon program, the network can perform authentication using any authentication scheme. For example, the authentication daemon could perform either a centralised authentication scheme or a Kerberos authentication scheme. Alternatively, the authentication daemon may simply just examine a file containing passwords.

As shown above, the authentication of remote users by servers can be performed in various ways.
 35 Under some circumstances, there is very little reason to be suspicious of requests arriving at a server and low cost authentication of remote users is justified. In other environments, servers must exercise greater vigilance. No one policy will be best for all cases. Therefore, this disclosed arrangement supports a range of authentication and authorisation policies.

40 Claims

1. A system having means for authenticating a requester, at a first node, of a service running at a second node, wherein the requester and the service are connected by a means of communication in a
 45 distributed data processing system, the system comprising:
 means for constructing authentication information by a facility, supporting an authentication policy, separate from the requester; and
 means for determining, at the second node, from the constructed authentication information, an authentication of the requester.

50 2. A system as claimed in claim 1 further comprising means, at the second node, for constructing a first authentication acknowledgement from the constructed authentication information and means for determining, at the first node, an authentication of the service from the constructed first authentication acknowledgement.

3. A system as claimed in Claim 2 further comprising means for constructing a second authentication
 55 acknowledgement at the first node during the construction of the authentication information, and means for comparing the first authentication acknowledgement with the second authentication acknowledgement for use by the determining means.

4. A system having means for authenticating a requester, at a first node, of a service running at a

second node, wherein the requester and the service are connected by a means of communication in a distributed data processing system, the system comprising:

means for constructing authentication information and an authentication acknowledgement by a facility, supporting an authentication policy, separate from the requester;

5 means for sending, by the requester, the authentication information to the service running at the second node;

means for processing the sent authentication information at a second facility, supporting the authentication policy, at the second node separate from the service;

10 means for acquiring, by the service, an outcome of the processing for determining a first authentication of the requester and a second authentication acknowledgement;

means for receiving, by the requester, the second authentication acknowledgement; and

means for comparing, by the requester, the first authentication acknowledgement and the second received authentication acknowledgement for determining a second authentication of the service.

5. A system as claimed in any preceding claim, further comprising means for replacing the current separate facility with a different separate facility supporting a different implementation of the authentication policy.

6. A system as claimed in any of claims 1 to 4, further comprising means for replacing the current separate facility with a different separate facility supporting a different authentication policy.

7. A system as claimed in any preceding claim, wherein the requester is a process running for a user on an operating system at the first node and the separate facility is a daemon process.

8. A system as claimed in claim 7 wherein the daemon process performs operations, to construct the authentication information, that the requesting process is incapable of performing at the time of the request.

9. A system as claimed in any of claims 1 to 6, wherein the requester is a process running on an operating system at the first node and the separate facility is accessible by at least one other process running on the operating system.

25 means for constructing authentication information and an authentication acknowledgement by a facility, supporting an authentication policy, separate from the requester;

means for sending, by the requester, the authentication information to the service running at the second node;

30 means for processing the sent authentication information at a second facility, supporting the authentication policy, at the second node separate from the service;

means for acquiring, by the service, an outcome of the processing for determining a first authentication of the requester and a second authentication acknowledgement;

means for receiving, by the requester, the second authentication acknowledgement; and

35 means for comparing, by the requester, the first authentication acknowledgement and the second received authentication acknowledgement for determining a second authentication of the service.

10. A method for authenticating a requester, at a first node, of a service running at a second node, wherein the requester and the service are connected by a means of communication in a distributed data processing system, the method comprising:

40 constructing authentication information by a facility, supporting an authentication policy, separate from the requester; and

determining, at the second node, from the constructed authentication information an authentication of the requester.

11. A method as claimed in Claim 10, further comprising constructing, at the second node, a first authentication acknowledgement from the constructed authentication information and determining, at the first node, an authentication of the service from the constructed first authentication acknowledgement.

12. A method as claimed in Claim 11, further comprising constructing a second authentication acknowledgement at the first node during the construction of the authentication information, and comparing the first authentication acknowledgement with the second authentication acknowledgement to determine the authentication of the service.

50 13. A method for authenticating a requester, at a first node, of a service running at a second node, wherein the requester and the service are connected by a means of communication in a distributed data processing system, the method comprising:

constructing authentication information and an authentication acknowledgement by a facility, supporting an authentication policy, separate from the requester;

55 sending, by the requester, the authentication information to the service running at the second node;

processing the sent authentication information at a second facility, supporting the authentication policy, at the second node separate from the service;

acquiring, by the service, an outcome of the processing for determining a first authentication of the requester and a second authentication acknowledgement;
 receiving, by the requester, the second authentication acknowledgement; and
 comparing, by the requester, the first authentication acknowledgement and the second received authentication acknowledgement for determining a second authentication of the service.

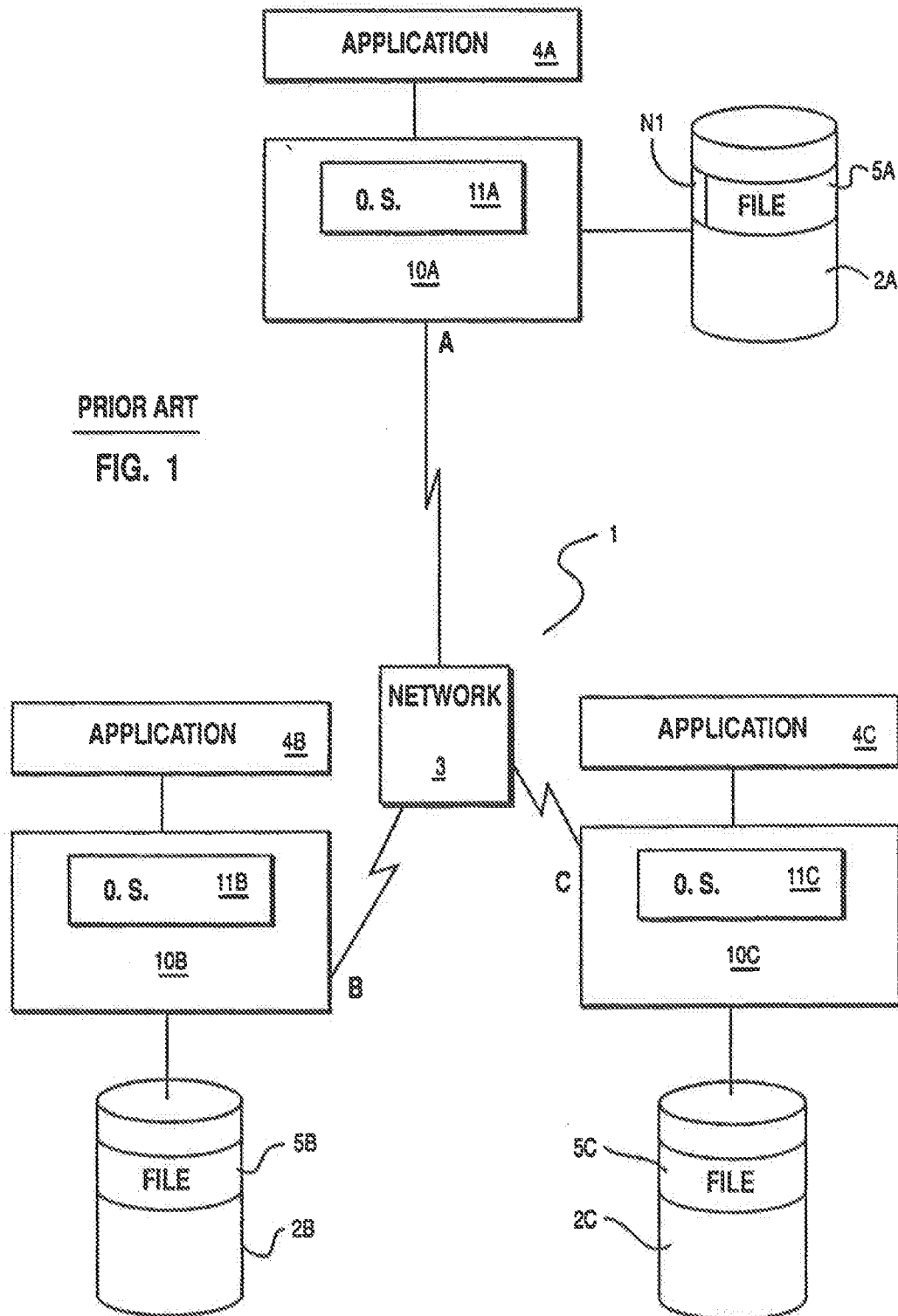
14. A method as claimed in any of Claims 10 to 13, further comprising replacing the first separate facility and the second separate facility with different separate mechanisms supporting a different authentication policy.

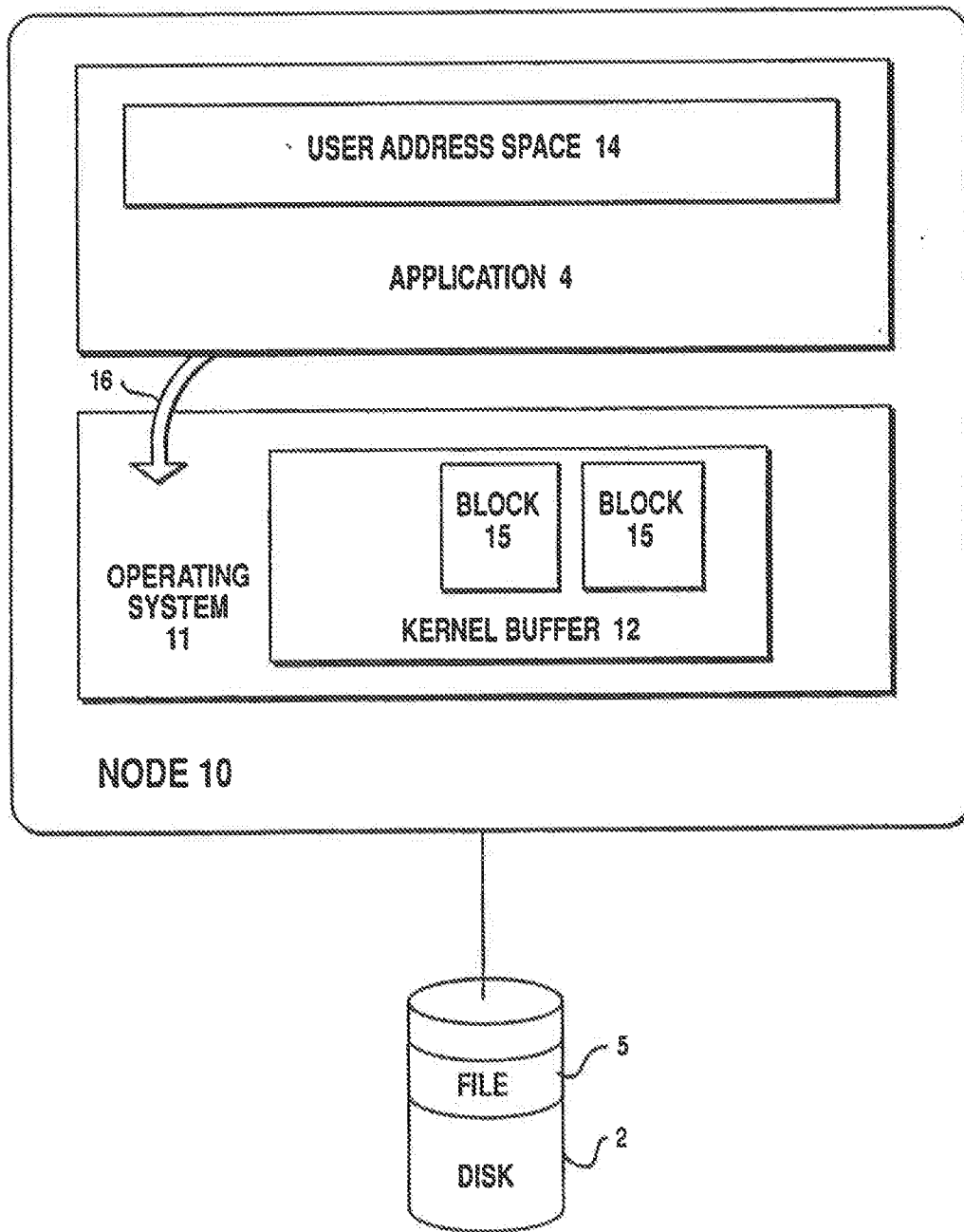
15. A method for use on a first data processing system having means for requesting, by a process at the first data processing system, a service at a second data processing system connected to the first data processing system through a means of communication, the method comprising:
 sending a message to a replaceable facility, supporting an authentication policy, separate from the requesting process, to initiate authentication by constructing authentication information; and
 sending, unaware of the contents of the constructed authentication information, the constructed authentication information, with a request to use the service, to the service for becoming authenticated to use the service.

16. A method as claimed in claim 15, further comprising receiving, from the service for the request, an acknowledgement having a first value, comparing the first value to a second value received from the replaceable facility, and determining the authentication of the service from the compared values.

17. A method for use on a second data processing system having means for receiving a request, from a process at the first data processing system, for a service, the second data processing system connected to the first data processing system through a means of communication, the method comprising:
 sending authentication information, received from the process, to a replaceable facility, supporting an authentication policy, separate from the service, for an interpretation of the authentication information and a construction of a plurality of authentication credentials;
 receiving the constructed credentials from the separate facility;
 performing an operation on the request based on the received credentials; and
 returning to the requesting process a result of the operation and the authentication acknowledgement received from the separate facility.

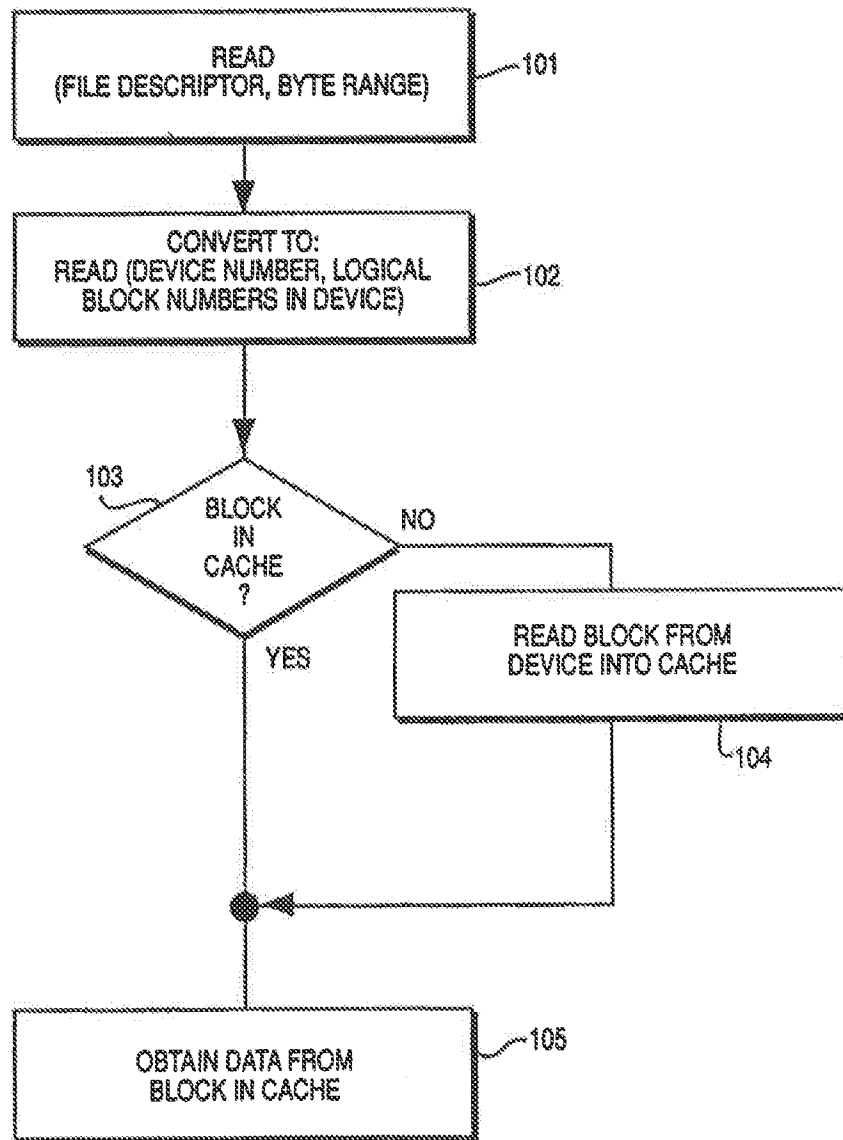
18. A method for use with at least one data processing system, the method comprising:
 receiving a message from a process to initiate authentication of the process in response to a request by the requesting process to use a service of a different process;
 constructing authentication information and an authentication acknowledgement from requester information and service information found in the received message;
 sending the constructed authentication information and the authentication acknowledgement to the requesting process;
 receiving the constructed authentication information from the service;
 constructing a plurality of credentials from the received authentication information for the service and a second authentication acknowledgement; and
 sending the constructed credentials and the authentication acknowledgement to the service.





PRIOR ART

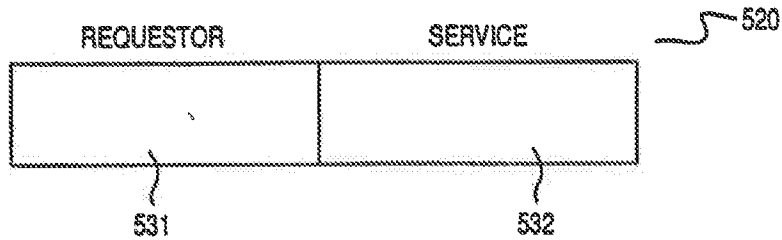
FIG. 2



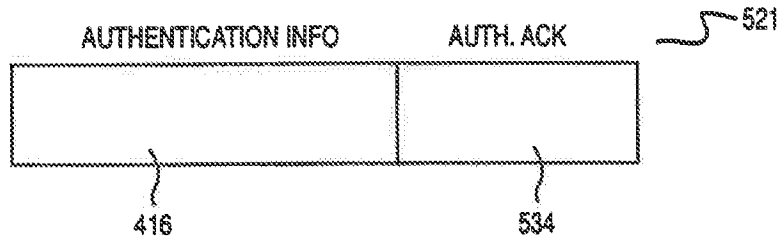
PRIOR ART

FIG. 3

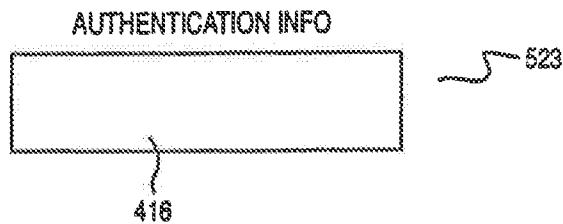
REQUESTOR TO AUTHENTICATION AGENT MESSAGE



AUTHENTICATION AGENT TO REQUESTOR MESSAGE



SERVICE TO AUTHENTICATION AGENT MESSAGE



AUTHENTICATION AGENT TO SERVICE MESSAGE

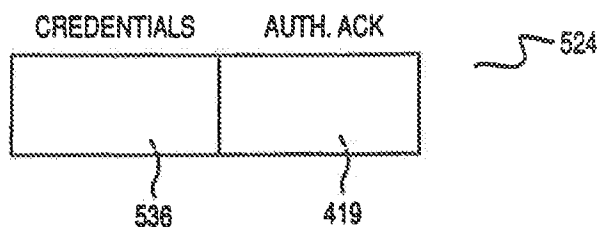


FIG. 4B

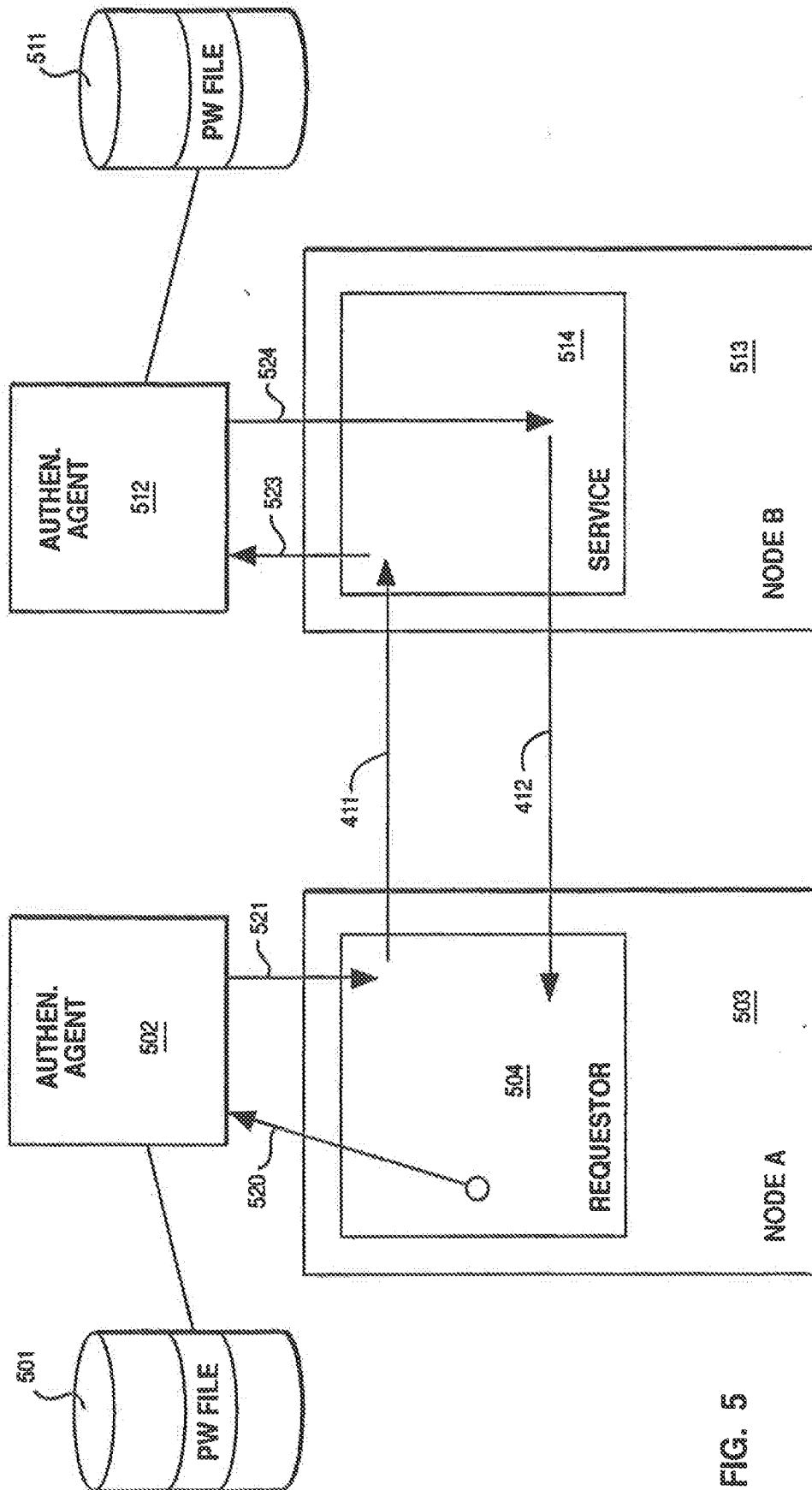


FIG. 5

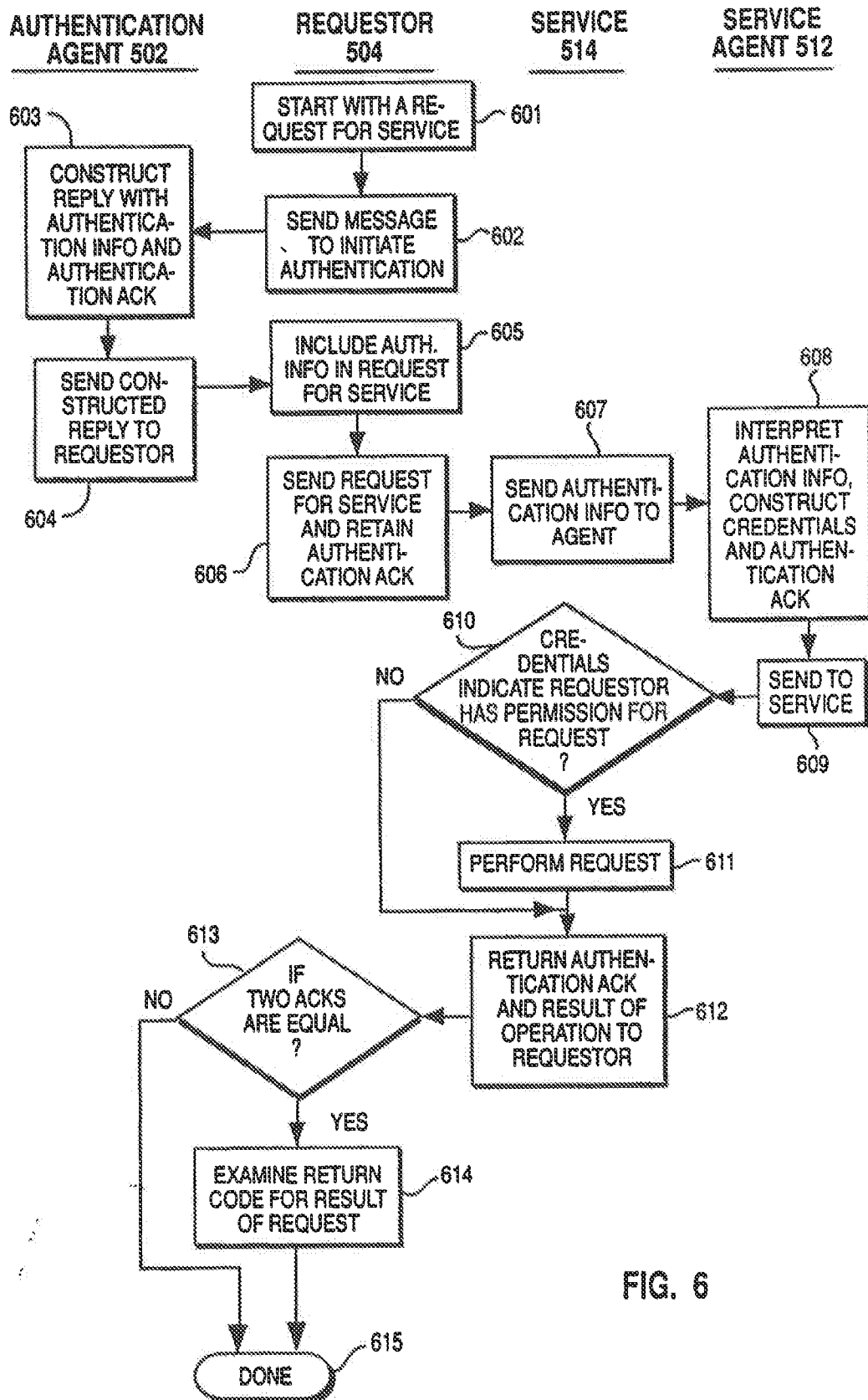


FIG. 6

Electronic Acknowledgement Receipt

EFS ID:	13866489
Application Number:	13585408
International Application Number:	
Confirmation Number:	4941
Title of Invention:	SYSTEM AND METHOD FOR DISTRIBUTING DIGITAL CONTENT TO BE RENDERED IN ACCORDANCE WITH USAGE RIGHTS INFORMATION
First Named Inventor/Applicant Name:	Mark J. Stefik
Customer Number:	98804
Filer:	Stephen M. Hertzler
Filer Authorized By:	
Attorney Docket Number:	10-510-US-C73
Receipt Date:	28-SEP-2012
Filing Date:	14-AUG-2012
Time Stamp:	17:32:31
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	Information Disclosure Statement (IDS) Form (SB08)	10-510-US-C73_-_2012-09-28_-_Information_Disclosure_Statement.pdf	612570 8416b17167191542e4ec980f117e5157ef630636	no	4

Warnings:

Information:

2	Foreign Reference	10-510-US-C73_-_2012-09-28_-_Foreign_Reference1.pdf	2690251 0912365a453b463efc0ff6b6712849206bc679f2	no	25
Warnings:					
Information:					
3	Foreign Reference	10-510-US-C73_-_2012-09-28_-_Foreign_Reference2.pdf	2465260 a39fb42488f0bd80fadd02b8bf95ce3dc8724d9b	no	21
Warnings:					
Information:					
4	Non Patent Literature	10-510-US-C73_-_2012-09-28_-_NPL.pdf	4921168 af1ff251bc0d7d75f5cceaaff67fe28d0a15c1ce5	no	18
Warnings:					
Information:					
Total Files Size (in bytes):			10689249		
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. <u>New Applications Under 35 U.S.C. 111</u> 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. <u>National Stage of an International Application under 35 U.S.C. 371</u> 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. <u>New International Application Filed with the USPTO as a Receiving Office</u> 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.					



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/585,408	08/14/2012	Mark J. Stefik	10-510-US-C73	4941
98804	7590	10/16/2012		
Reed Smith LLP P.O. Box 488 Pittsburgh, PA 15230			EXAMINER HOFFMAN, BRANDON S	
			ART UNIT 2433	PAPER NUMBER
			NOTIFICATION DATE 10/16/2012	DELIVERY MODE ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

ptoipinbox@reedsmith.com
mskaufman@reedsmith.com

Office Action Summary	Application No. 13/585,408	Applicant(s) STEFIK ET AL.	
	Examiner BRANDON HOFFMAN	Art Unit 2433	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 14 August 2012.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on ____; the restriction requirement and election have been incorporated into this action.
- 4) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 5) ☒ Claim(s) 1-15 is/are pending in the application.
- 5a) Of the above claim(s) ____ is/are withdrawn from consideration.
- 6) ☐ Claim(s) ____ is/are allowed.
- 7) ☒ Claim(s) 1-15 is/are rejected.
- 8) ☐ Claim(s) ____ is/are objected to.
- 9) ☐ Claim(s) ____ are subject to restriction and/or election requirement.

Application Papers

- 10) ☒ The specification is objected to by the Examiner.
- 11) ☒ The drawing(s) filed on 14 August 2012 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 12) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 13) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. ____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)	4) ☐ Interview Summary (PTO-413)
2) ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)	Paper No(s)/Mail Date. ____.
3) ☒ Information Disclosure Statement(s) (PTO/SB/08)	5) ☐ Notice of Informal Patent Application
Paper No(s)/Mail Date <u>9-21-12 / 9-28-12</u> .	6) ☐ Other: ____.

DETAILED ACTION

1. Claims 1-15 are pending in this office action.

Information Disclosure Statement

2. The information disclosure statements (IDS's) submitted on September 21, 2012, and September 28, 2012, are in compliance with the provisions of 37 CFR 1.97. Accordingly, the information disclosure statement is being considered by the examiner.

Specification

3. The disclosure is objected to because of the following informalities: the CROSS REFERENCE TO RELATED APPLICATIONS section needs to be updated to reflect applications that have been patented/abandoned. Appropriate correction is required.

Claim Objections

1. Claim 5 is objected to because of the following informalities: claim 5 claims to be dependent from claim 10. Appropriate correction is required.

Double Patenting

2. The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent

and to prevent possible harassment by multiple assignees. A nonstatutory obviousness-type double patenting rejection is appropriate where the conflicting claims are not identical, but at least one examined application claim is not patentably distinct from the reference claim(s) because the examined application claim is either anticipated by, or would have been obvious over, the reference claim(s). See, e.g., *In re Berg*, 140 F.3d 1428, 46 USPQ2d 1226 (Fed. Cir. 1998); *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); and *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) or 1.321(d) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent either is shown to be commonly owned with this application, or claims an invention made as a result of activities undertaken within the scope of a joint research agreement.

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

3. Claims 1-15 are rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 1-47 of U.S. Patent No. 6,898,576. Although the conflicting claims are not identical, they are not patentably distinct from

each other because application and patent both claim usage rights determining whether content may be rendered.

4. Claims 1-15 are provisionally rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 1-18 of copending Application No. 13/584,782. Although the conflicting claims are not identical, they are not patentably distinct from each other because both applications claim determining whether digital content may be rendered based on usage rights. The instant application further claims how the digital content may be rendered. It would have been obvious to add usage control on how the content may be used because some content should not be copied even though you have rights to view it.

This is a provisional obviousness-type double patenting rejection because the conflicting claims have not in fact been patented.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to BRANDON HOFFMAN whose telephone number is (571)272-3863. The examiner can normally be reached on M-F 8:30 - 5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Jeffrey C. Pwu can be reached on 571-272-6798. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Art Unit: 2433

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Brandon S Hoffman/
Primary Examiner, Art Unit 2433

Search Notes 	Application/Control No. 13585408	Applicant(s)/Patent Under Reexamination STEFIK ET AL.
	Examiner BRANDON HOFFMAN	Art Unit 2433

SEARCHED			
Class	Subclass	Date	Examiner
726	29 - with keyword limiters	10-9-12	BH

SEARCH NOTES		
Search Notes	Date	Examiner
inventor name search	10-9-12	BH
see attached EAST search notes	10-9-12	BH

INTERFERENCE SEARCH			
Class	Subclass	Date	Examiner

	/BRANDON HOFFMAN/ Primary Examiner.Art Unit 2433

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		13585408
	Filing Date		2012-08-14
	First Named Inventor	Mark J. Stefik	
	Art Unit	2431	
	Examiner Name		
	Attorney Docket Number	10-510-US-C73	

U.S.PATENTS						Remove
Examiner Initial*	Cite No	Patent Number	Kind Code ¹	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	5204961		1993-04-20	Barlow	
	2	4817140		1989-03-28	Chandra et al.	
	3	5390297		1995-02-14	Barber et al.	
	4	6135646		2000-10-24	Kahn et al.	

If you wish to add additional U.S. Patent citation information please click the Add button.

Add

U.S.PATENT APPLICATION PUBLICATIONS						Remove
Examiner Initial*	Cite No	Publication Number	Kind Code ¹	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Published Application citation information please click the Add button.

Add

FOREIGN PATENT DOCUMENTS								Remove
Examiner Initial*	Cite No	Foreign Document Number ³	Country Code ²	Kind Code ⁴	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T ⁵

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		13585408	13585408 - GAU: 2433
	Filing Date		2012-08-14	
	First Named Inventor	Mark J. Stefik		
	Art Unit	2431		
	Examiner Name			
	Attorney Docket Number	10-510-US-C73		

	1	0588415	EP	A1	1994-03-23	Huss, et al.		☐
	2	0398492	EP	A2	1990-11-22	Loucks, et al.		☐

If you wish to add additional Foreign Patent Document citation information please click the Add button **Add**

NON-PATENT LITERATURE DOCUMENTS

Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T ⁵
	1	KOHL, JOHN T. et al., "The Evolution of the Kerberos Authentication Service", Distributed Open Systems, IEEE, 1994, 18 pages.	☐

If you wish to add additional non-patent literature document citation information please click the Add button **Add**

EXAMINER SIGNATURE

Examiner Signature	/Brandon Hoffman/	Date Considered	10/09/2012

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

¹ See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. ² Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). ³ For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. ⁴ Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. ⁵ Applicant is to place a check mark here if English language translation is attached.

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	13585408	13585408 - GAU: 2433
Filing Date	2012-08-14	
First Named Inventor	Mark J. Stefik	
Art Unit	2431	
Examiner Name		
Attorney Docket Number	10-510-US-C73	

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

☐ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

☐ See attached certification statement.

☐ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Stephen M. Hertzler, Reg. No. 58,247/	Date (YYYY-MM-DD)	2012-09-28
Name/Print	Stephen M. Hertzler	Registration Number	58,247

This collection of information is required by 37 CFR 1.97 and 1.98. 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 1.14. This collection is estimated to take 1 hour 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.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these records.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	1227	(726/29).CCLS.	US-PGPUB; USPAT; USOCR	OR	OFF	2012/10/09 13:48
L2	209	(STEFIK near MARK PIROLI near PETER).in.	US-PGPUB; USPAT; USOCR	OR	OFF	2012/10/09 13:49
L3	4	("4817140" "5204961" "5390297" "6135646").PN.	US-PGPUB; USPAT; USOCR	OR	OFF	2012/10/09 13:50
L4	102095	trust\$3	US-PGPUB; USPAT; USOCR	OR	OFF	2012/10/09 13:51
L5	2359	usage adj rights	US-PGPUB; USPAT; USOCR	OR	OFF	2012/10/09 14:04
L7	249736	authentic\$5	US-PGPUB; USPAT; USOCR	OR	OFF	2012/10/09 14:05
L8	1324520	render\$3	US-PGPUB; USPAT; USOCR	OR	OFF	2012/10/09 14:14
L9	760	4 and 5 and 7 and 8	US-PGPUB; USPAT; USOCR	OR	OFF	2012/10/09 14:35
L10	34	1 and 9	US-PGPUB; USPAT; USOCR	OR	OFF	2012/10/09 14:36
L11	113	2 and 9	US-PGPUB; USPAT; USOCR	OR	OFF	2012/10/09 14:36
L12	0	10 and @ad<"19941123"	US-PGPUB; USPAT; USOCR	OR	OFF	2012/10/09 15:18
L13	0	9 and @ad<"19941123"	US-PGPUB; USPAT; USOCR	OR	OFF	2012/10/09 15:18
L14	5	9 and @ad<"19951123"	US-PGPUB; USPAT; USOCR	OR	OFF	2012/10/09 15:35
L15	1	("6898576").PN.	US-PGPUB; USPAT; USOCR	OR	OFF	2012/10/09 16:48

10/ 9/ 2012 5:09:08 PM

C:\ Users\ bhoffman\ Documents\ EAST\ Workspaces\ 13585408.wsp



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
 United States Patent and Trademark Office
 Address: COMMISSIONER FOR PATENTS
 P.O. Box 1450
 Alexandria, Virginia 22313-1450
 www.uspto.gov

BIB DATA SHEET

CONFIRMATION NO. 4941

SERIAL NUMBER	FILING or 371(c) DATE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.		
13/585,408	08/14/2012	726	2433	10-510-US-C73		
RULE						
APPLICANTS Mark J. Stefik, Portola Valley, CA; Peter L.T. Pirolli, San Francisco, CA; ** CONTINUING DATA ***** This application is a CON of 13/584,782 08/13/2012 * which is a CON of 11/304,793 12/16/2005 ABN which is a DIV of 11/135,352 05/24/2005 PAT 7,266,529 which is a CON of 10/322,759 12/19/2002 PAT 6,898,576 which is a CON of 09/778,001 02/07/2001 PAT 6,708,157 which is a DIV of 08/967,084 11/10/1997 PAT 6,236,971 which is a CON of 08/344,760 11/23/1994 ABN (*)Data provided by applicant is not consistent with PTO records. ** FOREIGN APPLICATIONS ***** ** IF REQUIRED, FOREIGN FILING LICENSE GRANTED ** 08/22/2012						
Foreign Priority claimed ☐ Yes ☒ No 35 USC 119(a-d) conditions met ☐ Yes ☒ No Verified and /BRANDON S Hoffmann/ Acknowledged Examiner's Signature		☐ Met after Allowance Initials	STATE OR COUNTRY CA	SHEETS DRAWINGS 13	TOTAL CLAIMS 15	INDEPENDENT CLAIMS 3
ADDRESS Reed Smith LLP P.O. Box 488 Pittsburgh, PA 15230 UNITED STATES						
TITLE SYSTEM AND METHOD FOR DISTRIBUTING DIGITAL CONTENT TO BE RENDERED IN ACCORDANCE WITH USAGE RIGHTS INFORMATION						
FILING FEE RECEIVED 1550	FEES: Authority has been given in Paper No. _____ to charge/credit DEPOSIT ACCOUNT No. _____ for following:			☐ All Fees ☐ 1.16 Fees (Filing) ☐ 1.17 Fees (Processing Ext. of time) ☐ 1.18 Fees (Issue) ☐ Other _____ ☐ Credit		

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		13585408	
	Filing Date		2012-08-14	
	First Named Inventor	Mark J. STEFIK		
	Art Unit	2431		
	Examiner Name			
	Attorney Docket Number	10-510-US-C73		

U.S.PATENTS						Remove
Examiner Initial*	Cite No	Patent Number	Kind Code ¹	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Patent citation information please click the Add button.

Add

U.S.PATENT APPLICATION PUBLICATIONS						Remove
Examiner Initial*	Cite No	Publication Number	Kind Code ¹	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Published Application citation information please click the Add button.

Add

FOREIGN PATENT DOCUMENTS							Remove	
Examiner Initial*	Cite No	Foreign Document Number ³	Country Code ²	Kind Code ⁴	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T ⁵
	1							☐

If you wish to add additional Foreign Patent Document citation information please click the Add button

Add

NON-PATENT LITERATURE DOCUMENTS			Remove
Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T ⁵

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		13585408	13585408 - GAU: 2433
	Filing Date		2012-08-14	
	First Named Inventor	Mark J. STEFIK		
	Art Unit	2431		
	Examiner Name			
	Attorney Docket Number	10-510-US-C73		

1	Non-Final Office Action dated June 12, 2008 cited in Application No. 11/304,793.	☐
2	Final Office Action dated November 14, 2008 cited in Application No. 11/304,793.	☐
3	Non- Final Office Action dated May 27, 2009 cited in Application No. 11/304,793.	☐
4	Final Office Action dated January 22, 2010 cited in Application No. 11/304,793.	☐
5	Decision on Appeal dated June 13, 2012 cited in Application No. 11/304,793.	☐

If you wish to add additional non-patent literature document citation information please click the Add button **Add**

EXAMINER SIGNATURE

Examiner Signature	/Brandon Hoffman/	Date Considered	10/09/2012

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

¹ See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. ² Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). ³ For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. ⁴ Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. ⁵ Applicant is to place a check mark here if English language translation is attached.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		13585408	13585408 - GAU: 2433
	Filing Date		2012-08-14	
	First Named Inventor	Mark J. STEFIK		
	Art Unit	2431		
	Examiner Name			
	Attorney Docket Number	10-510-US-C73		

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

☐ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

☐ See attached certification statement.

☐ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Stephen M. Hertzler, Reg. No. 58,247/	Date (YYYY-MM-DD)	2012-09-21
Name/Print	Stephen M. Hertzler	Registration Number	58,247

This collection of information is required by 37 CFR 1.97 and 1.98. 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 1.14. This collection is estimated to take 1 hour 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.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these records.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

<i>Index of Claims</i> 	Application/Control No. 13585408	Applicant(s)/Patent Under Reexamination STEFIK ET AL.
	Examiner BRANDON HOFFMAN	Art Unit 2433

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant		☐ CPA		☐ T.D.		☐ R.1.47			
CLAIM		DATE							
Final	Original	10/09/2012							
	1	✓							
	2	✓							
	3	✓							
	4	✓							
	5	✓							
	6	✓							
	7	✓							
	8	✓							
	9	✓							
	10	✓							
	11	✓							
	12	✓							
	13	✓							
	14	✓							
	15	✓							

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:	)	Confirmation No. 4941
Mark J. Stefik, et al.	)	Group Art Unit: 2433
Serial No. 13/585,408	)	Examiner: Hoffman, Brandon S
Filed: August 14, 2012	)	
For: SYSTEM AND METHOD FOR	)	Date: November 5, 2012
DISTRIBUTING DIGITAL CONTENT	)	
TO BE RENDERED IN ACCORDANCE	)	
WITH USAGE RIGHTS	)	
INFORMATION	)	

RESPONSE TO OFFICE ACTION

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

In response to the Office Action mailed October 16, 2012, Applicants submit the following remarks. Applicants respectfully request reconsideration and allowance of this application.

A Listing of the Claims begins on page 2 of this paper.

Remarks begin on page 7 of this paper.

Listing of the Claims:

1. (Original) A computer-implemented method of distributing digital content to at least one recipient computing device to be rendered by the at least one recipient computing device in accordance with usage rights information, the method comprising:

determining, by at least one sending computing device, if the at least one recipient computing device is trusted to receive the digital content from the at least one sending computing device;

sending the digital content, by the at least one sending computing device, to the at least one recipient computing device only if the at least one recipient computing device has been determined to be trusted to receive the digital content from the at least one sending computing device; and

sending usage rights information indicating how the digital content may be rendered by the at least one recipient computing device, the usage rights information being enforceable by the at least one recipient computing device.

2. (Original) The method of claim 1, wherein the usage rights information further includes a condition under which the content can be rendered.

3. (Original) The method of claim 1, wherein the determination of trust comprises:

receiving a request from at least one recipient computing device for an authorization object required to render the digital content; and

transmitting the authorization object to the at least one recipient computing device when it is determined that the request should be granted.

4. (Original) The method of claim 1, wherein the determination of trust comprises:

receiving a registration message from the at least one recipient device, the registration message including an identification certificate of the recipient computing device and a random registration identifier, the identification certificate being certified by a master device;

validating the authenticity of the at least one recipient device;

exchanging messages including at least one session key with the at least one recipient device, the session key to be used in communications; and

conducting a secure transaction using the session key, wherein the secure transaction includes sending the digital content to the at least one recipient device.

5. (Currently Amended) The method of claim 1 [[10]], wherein the validating comprises:
- verifying the identification certificate of the at least one recipient device;
 - generating a message to test the authenticity of the at least one recipient device, the generated message including a nonce;
 - sending the generated message to the at least one recipient device; and
 - verifying if the at least one recipient device correctly processed the generated message.

6. (Original) A sending apparatus for distributing digital content to at least one recipient computing device to be rendered by the at least one recipient computing device in accordance with usage rights information, the sending apparatus comprising:

- one or more processors; and

- one or more memories operatively coupled to at least one of the one or more processors and having instructions stored thereon that, when executed by at least one of the one or more processors, cause at least one of the one or more processors to:

- determine if the at least one recipient computing device is trusted to receive the digital content from the sending apparatus;

- send the digital content, by the sending apparatus, to the at least one recipient computing device only if the at least one recipient computing device has been determined to be trusted to receive the digital content from the sending apparatus; and

- send usage rights information indicating how the digital content may be rendered by the at least one recipient computing device, the usage rights information being enforceable by the at least one recipient computing device.

7. (Original) The apparatus of claim 6, wherein the usage rights information further includes a condition under which the content can be rendered.

8. (Original) The apparatus of claim 6, wherein the determination of trust comprises:
receiving a request from at least one recipient computing device for an authorization object required to render the digital content; and
transmitting the authorization object to the at least one recipient computing device when it is determined that the request should be granted.
9. (Original) The apparatus of claim 6, wherein the determination of trust comprises:
receiving a registration message from the at least one recipient device, the registration message including an identification certificate of the recipient computing device and a random registration identifier, the identification certificate being certified by a master device;
validating the authenticity of the at least one recipient device;
exchanging messages including at least one session key with the at least one recipient device, the session key to be used in communications; and
conducting a secure transaction using the session key, wherein the secure transaction includes sending the digital content to the at least one recipient device.
10. (Original) The apparatus of claim 9, wherein the validating comprises:
verifying the identification certificate of the at least one recipient device;
generating a message to test the authenticity of the at least one recipient device, the generated message including a nonce;
sending the generated message to the at least one recipient device; and
verifying if the at least one recipient device correctly processed the generated message.
11. (Original) At least one non-transitory computer-readable medium storing computer-readable instructions that, when executed by at least one sending computing device, cause the at least one sending computing device to:
determine if the at least one recipient computing device is trusted to receive the digital content from the at least one sending computing device;

send the digital content, by the at least one sending computing device, to the at least one recipient computing device only if the at least one recipient computing device has been determined to be trusted to receive the digital content from the at least one sending computing device; and

send usage rights information indicating how the digital content may be rendered by the at least one recipient computing device, the usage rights information being enforceable by the at least on recipient computing device.

12. (Original) The at least one non-transitory computer-readable medium of claim 11, wherein the usage rights information further includes a condition under which the content can be rendered.

13. (Original) The at least one non-transitory computer-readable medium of claim 11, wherein the determination of trust comprises:

receiving a request from at least one recipient computing device for an authorization object required to render the digital content; and

transmitting the authorization object to the at least one recipient computing device when it is determined that the request should be granted.

14. (Original) The at least one non-transitory computer-readable medium of claim 11, wherein the determination of trust comprises:

receiving a registration message from the at least one recipient device, the registration message including an identification certificate of the recipient computing device and a random registration identifier, the identification certificate being certified by a master device;

validating the authenticity of the at least one recipient device;

exchanging messages including at least one session key with the at least one recipient device, the session key to be used in communications; and

conducting a secure transaction using the session key, wherein the secure transaction includes sending the digital content to the at least one recipient device.

15. (Original) The at least one non-transitory computer-readable medium of claim 14, wherein the validating comprises:

- verifying the identification certificate of the at least one recipient device;
- generating a message to test the authenticity of the at least one recipient device, the generated message including a nonce;
- sending the generated message to the at least one recipient device; and
- verifying if the at least one recipient device correctly processed the generated message.

REMARKS

Claims 1-15 are pending in this application, and claim 5 is amended herein. In view of the above amendments and the following remarks, Applicants request reconsideration and allowance of this application.

Objections to the Specification

The Examiner has objected to the cross reference section of the specification as failing to identify each referenced application as being patented or abandoned. However, the noted section of the specification clearly identifies the status of each referenced application as shown below:

- U.S. Application No. 13/584,782, filed August 13, 2012;
- U.S. Application No. 11/304,793, filed December 16, 2005;
- U.S. Application No. 11/135,352, U.S. Patent No. 7,266,529;
- U.S. Application No. 10/322,759, U.S. Patent No. 6,898,576;
- U.S. Application No. 09/778,001, U.S. Patent No. 6,708,157;
- U.S. Application No. 08/967,084, U.S. Patent No. 6,236,971; and
- U.S. Application No. 08/344,760, abandoned.

The status of the '782 and '793 applications are not included as these applications are currently pending. Thus, Applicants believe this section of the specification is correct, and request that this objection be withdrawn. If further clarification is required, Applicants request that the Examiner contact the undersigned.

Claim Objections

Claim 5 stands objected to as incorrectly stating a dependency on claim 10 rather than claim 1. Claim 5 is amended herein to correctly depend on claim 1. Thus, this objection should be withdrawn.

Double Patenting over U.S. Pat. No. 6,898,576

Claims 1-15 stand rejected on the ground of nonstatutory obviousness-type double patenting over claims 1-47 of U.S. Patent No. 6,898,576. Claim 1 of the '576 patent recites:

1. A method for enforcing execution of executable code in accordance with usage rights, said method comprising;

receiving a request to execute the executable code;

determining at a non-centralized repository, based on usage rights associated with the executable code, whether the request should be granted, the usage rights including a manner of indicating a specific instance of how the executable code can be executed; and

executing the executable code on a computing device in accordance with the manner of use if the result of said determining step is that the request should be granted,

wherein said request is generated by a requester device, said executing step is accomplished by a remote server that is remote from said requester device and said determining step is accomplished by a processing server comprising the non-centralized repository,

said requester device and said remote server communicate using a transmission protocol and wherein said executing step comprises executing the executable code in an address space of the remote server and permitting the requester device to access the executable code only through the transmission protocol,

said requesting step and said executing step are accomplished through an external interface of said remote server which provides for network connectivity between the remote server and the requester device using the transmission protocol,

the executable code comprises plural components, each of the components having a usage right associated therewith, said determining step comprising determining based on usage right associated with at least one component, whether the request should be granted, and said executing step comprising executing the component if the result of said determining step is that the request should be granted,

said determining step comprises accomplishing one or more transactions with respect to the executable code, and

said transactions in said accomplishing step comprise copy, transfer, loan, play, print, backup, restore, delete, directory, folder, extract, embed, edit, authorization, install, and uninstall transactions.

However, as was discussed with the Examiner during a recent telephone interview, the claims of the '576 patent clearly fail to recite determining whether the at least one recipient computing device is trusted to receive the digital content. Specifically, as recited in claim 1, *"determining, by at least one sending computing device, if the at least one recipient computing device is trusted to receive the digital content from the at least one sending computing device."* Similarly, as recited in claim 6, *"determine if the at least one recipient computing device is trusted to receive the digital content from the sending apparatus."* Finally, as recited in claim

11, “determine if the at least one recipient computing device is trusted to receive the digital content from the at least one sending computing device.” Thus, as was agreed by the Examiner during the interview, the double patenting rejection in view of the ‘576 patent should clearly be withdrawn.

Double Patenting over U.S. Appl. No. 13/584,782

Claims 1-15 stand provisionally rejected on the ground of nonstatutory obviousness-type double patenting over claims 1-18 of U.S. Appl. No. 13/584,782. Pursuant to MPEP 804, if “provisional” ODP rejections in two applications are the only rejections remaining in those applications, the examiner should withdraw the ODP rejection in the earlier filed application thereby permitting that application to issue without need of a terminal disclaimer. A terminal disclaimer must be required in the later-filed application before the ODP rejection can be withdrawn and the application permitted to issue. In the present case, the ‘782 application was filed on August 13, 2012, and this application was filed on August 14, 2012. Since this is the “later-filed application” of the two applications, Applicants will file a Terminal Disclaimer over the ‘782 application, if appropriate, when this application is otherwise in condition for allowance.

In view of the foregoing, Applicants request that the outstanding objections and rejections be withdrawn, and submit that this application is in condition for allowance, pending a possible terminal disclaimer filing over the ‘782 application. While no fees are believed to be due in connection with this filing, the Commissioner is hereby authorized to charge fees and credit overpayments to Deposit Account No. 50-1529. If any further information is needed, please contact the undersigned.

Date: November 5, 2012

REED SMITH LLP
CUSTOMER NO.: 98804
1301 K Street N.W.
Suite 1100 – East Tower
Washington, D.C. 20005

Respectfully submitted,
/Stephen M. Hertzler, Reg. No. 58,247/
Stephen M. Hertzler
Registration No. 58,247

Electronic Acknowledgement Receipt

EFS ID:	14151742
Application Number:	13585408
International Application Number:	
Confirmation Number:	4941
Title of Invention:	SYSTEM AND METHOD FOR DISTRIBUTING DIGITAL CONTENT TO BE RENDERED IN ACCORDANCE WITH USAGE RIGHTS INFORMATION
First Named Inventor/Applicant Name:	Mark J. Stefik
Customer Number:	98804
Filer:	Stephen M. Hertzler
Filer Authorized By:	
Attorney Docket Number:	10-510-US-C73
Receipt Date:	05-NOV-2012
Filing Date:	14-AUG-2012
Time Stamp:	16:37:33
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	Amendment/Req. Reconsideration-After Non-Final Reject	10-510-US-C73_-_2012-11-05_-_Response_to_Office_Action.pdf	531218 b96a5f3d4761c7ddc5ed267fcdc1fea83f5cc7c7	no	9

Warnings:

Information:

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.

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.

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875					Application or Docket Number 13/585,408		Filing Date 08/14/2012		☐ To be Mailed							
APPLICATION AS FILED – PART I																
(Column 1)			(Column 2)			SMALL ENTITY ☐		OR		OTHER THAN SMALL ENTITY						
FOR		NUMBER FILED		NUMBER EXTRA		RATE (\$)		FEE (\$)		RATE (\$)		FEE (\$)				
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))		N/A		N/A		N/A				N/A						
☐ SEARCH FEE (37 CFR 1.16(k), (l), or (m))		N/A		N/A		N/A				N/A						
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))		N/A		N/A		N/A				N/A						
TOTAL CLAIMS (37 CFR 1.16(j))		minus 20 =		*		X \$ =				X \$ =						
INDEPENDENT CLAIMS (37 CFR 1.16(h))		minus 3 =		*		X \$ =				X \$ =						
☐ APPLICATION SIZE FEE (37 CFR 1.16(s))		If the specification and drawings exceed 100 sheets of paper, the application size fee due is \$250 (\$125 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).														
☐ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))																
* If the difference in column 1 is less than zero, enter "0" in column 2.																
APPLICATION AS AMENDED – PART II																
(Column 1)			(Column 2)			(Column 3)			SMALL ENTITY		OR		OTHER THAN SMALL ENTITY			
AMENDMENT	11/05/2012		CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR		PRESENT EXTRA		RATE (\$)		ADDITIONAL FEE (\$)		RATE (\$)		ADDITIONAL FEE (\$)	
	Total (37 CFR 1.16(i))		* 15		Minus ** 20		= 0		X \$ =				OR X \$62=		0	
	Independent (37 CFR 1.16(h))		* 3		Minus *** 3		= 0		X \$ =				OR X \$250=		0	
	☐ Application Size Fee (37 CFR 1.16(s))															
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))															
	TOTAL ADD'L FEE															
OR																
TOTAL ADD'L FEE 0																
(Column 1)			(Column 2)			(Column 3)			SMALL ENTITY		OR		OTHER THAN SMALL ENTITY			
AMENDMENT			CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR		PRESENT EXTRA		RATE (\$)		ADDITIONAL FEE (\$)		RATE (\$)		ADDITIONAL FEE (\$)	
	Total (37 CFR 1.16(i))		*		Minus **		=		X \$ =				OR X \$ =			
	Independent (37 CFR 1.16(h))		*		Minus ***		=		X \$ =				OR X \$ =			
	☐ Application Size Fee (37 CFR 1.16(s))															
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))															
	TOTAL ADD'L FEE															
OR																
TOTAL ADD'L FEE																
* If the entry in column 1 is less than the entry in column 2, write "0" in column 3. ** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20". *** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3". The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.																

Legal Instrument Examiner:
/MONIQUE BRUNSON/

This collection of information is required by 37 CFR 1.16. 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 1.14. 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.**

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



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/585,408	08/14/2012	Mark J. Stefik	10-510-US-C73	4941
98804	7590	12/04/2012		
Reed Smith LLP P.O. Box 488 Pittsburgh, PA 15230			EXAMINER HOFFMAN, BRANDON S	
			ART UNIT 2433	PAPER NUMBER
			NOTIFICATION DATE 12/04/2012	DELIVERY MODE ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

ptoipinbox@reedsmith.com
mskaufman@reedsmith.com

Office Action Summary	Application No. 13/585,408	Applicant(s) STEFIK ET AL.	
	Examiner BRANDON HOFFMAN	Art Unit 2433	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 05 November 2012.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on ____; the restriction requirement and election have been incorporated into this action.
- 4) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 5) ☒ Claim(s) 1-15 is/are pending in the application.
- 5a) Of the above claim(s) ____ is/are withdrawn from consideration.
- 6) ☐ Claim(s) ____ is/are allowed.
- 7) ☒ Claim(s) 1-15 is/are rejected.
- 8) ☐ Claim(s) ____ is/are objected to.
- 9) ☐ Claim(s) ____ are subject to restriction and/or election requirement.

* If any claims have been determined allowable, you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to PPHfeedback@uspto.gov.

Application Papers

- 10) ☐ The specification is objected to by the Examiner.
- 11) ☐ The drawing(s) filed on ____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. ____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)	3) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. ____.
2) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date ____.	4) ☐ Other: ____.

DETAILED ACTION

1. Claims 1-15 are pending in this office action.

Double Patenting

1. The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the “right to exclude” granted by a patent and to prevent possible harassment by multiple assignees. A nonstatutory obviousness-type double patenting rejection is appropriate where the conflicting claims are not identical, but at least one examined application claim is not patentably distinct from the reference claim(s) because the examined application claim is either anticipated by, or would have been obvious over, the reference claim(s). See, e.g., *In re Berg*, 140 F.3d 1428, 46 USPQ2d 1226 (Fed. Cir. 1998); *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); and *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) or 1.321(d) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent either is shown to be commonly owned with this application, or claims an invention made as a result of activities undertaken within the scope of a joint research agreement.

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

2. Claims 1-15 are provisionally rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 1-18 of copending Application No. 13/584,782. Although the conflicting claims are not identical, they are not patentably distinct from each other because both applications claim determining whether digital content may be rendered based on usage rights. The instant application further claims how the digital content may be rendered. It would have been obvious to add usage control on how the content may be used because some content should not be copied even though you have rights to view it.

This is a provisional obviousness-type double patenting rejection because the conflicting claims have not in fact been patented. The copending case has a notice of allowance, dated November 27, 2012.

Conclusion

1. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the

Art Unit: 2433

shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to BRANDON HOFFMAN whose telephone number is (571)272-3863. The examiner can normally be reached on M-F 8:30 - 5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Jeffrey C. Pwu can be reached on 571-272-6798. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Brandon S Hoffman/
Primary Examiner, Art Unit 2433

EAST Search History**EAST Search History (Prior Art)**

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	103872	trust\$3	US-PGPUB; USPAT; USOCR	OR	OFF	2012/11/27 16:44
L2	655828	sender sending	US-PGPUB; USPAT; USOCR	OR	OFF	2012/11/27 16:44
L3	1031087	recipient receiver	US-PGPUB; USPAT; USOCR	OR	OFF	2012/11/27 16:44
L4	4326	usage with rights	US-PGPUB; USPAT; USOCR	OR	OFF	2012/11/27 16:44
L5	1338633	render\$	US-PGPUB; USPAT; USOCR	OR	OFF	2012/11/27 16:44
L6	691	1 and 2 and 3 and 4 and 5	US-PGPUB; USPAT; USOCR	OR	OFF	2012/11/27 16:44
L8	0	6 and @ad<"19941123"	US-PGPUB; USPAT; USOCR	OR	OFF	2012/11/27 16:45
S1	1227	(726/29).CCLS.	US-PGPUB; USPAT; USOCR	OR	OFF	2012/10/09 13:48
S2	209	(STEFIK near MARK PIROLI near PETER).in.	US-PGPUB; USPAT; USOCR	OR	OFF	2012/10/09 13:49
S3	4	("4817140" "5204961" "5390297" "6135646").PN.	US-PGPUB; USPAT; USOCR	OR	OFF	2012/10/09 13:50
S4	102095	trust\$3	US-PGPUB; USPAT; USOCR	OR	OFF	2012/10/09 13:51
S5	2359	usage adj rights	US-PGPUB; USPAT; USOCR	OR	OFF	2012/10/09 14:04
S6	249736	authentic\$5	US-PGPUB; USPAT; USOCR	OR	OFF	2012/10/09 14:05
S7	1324520	render\$3	US-PGPUB; USPAT; USOCR	OR	OFF	2012/10/09 14:14
S8	760	S4 and S5 and S6 and S7	US-PGPUB; USPAT; USOCR	OR	OFF	2012/10/09 14:35
S9	34	S1 and S8	US-PGPUB; USPAT; USOCR	OR	OFF	2012/10/09 14:36
S10	113	S2 and S8	US-PGPUB; USPAT; USOCR	OR	OFF	2012/10/09 14:36
S11	0	S9 and @ad<"19941123"	US-PGPUB; USPAT; USOCR	OR	OFF	2012/10/09 15:18
S12	0	S8 and @ad<"19941123"	US-PGPUB; USPAT; USOCR	OR	OFF	2012/10/09 15:18
S13	5	S8 and @ad<"19951123"	US-PGPUB; USPAT; USOCR	OR	OFF	2012/10/09 15:35
S14	1	("6898576").PN.	US-PGPUB; USPAT; USOCR	OR	OFF	2012/10/09 16:48

11/27/2012 4:45:28 PM**C:\Users\bhoffman\Documents\EAST\Workspaces\13585408.wsp**

<i>Index of Claims</i> 	Application/Control No. 13585408	Applicant(s)/Patent Under Reexamination STEFIK ET AL.
	Examiner BRANDON HOFFMAN	Art Unit 2433

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant				☐ CPA		☐ T.D.		☐ R.1.47	
CLAIM		DATE							
Final	Original	10/09/2012	11/27/2012						
	1	✓	✓						
	2	✓	✓						
	3	✓	✓						
	4	✓	✓						
	5	✓	✓						
	6	✓	✓						
	7	✓	✓						
	8	✓	✓						
	9	✓	✓						
	10	✓	✓						
	11	✓	✓						
	12	✓	✓						
	13	✓	✓						
	14	✓	✓						
	15	✓	✓						

Search Notes 	Application/Control No. 13585408	Applicant(s)/Patent Under Reexamination STEFIK ET AL.
	Examiner BRANDON HOFFMAN	Art Unit 2433

SEARCHED			
Class	Subclass	Date	Examiner
726	29 - with keyword limiters	10-9-12	BH

SEARCH NOTES		
Search Notes	Date	Examiner
inventor name search	10-9-12	BH
see attached EAST search notes	10-9-12	BH
updated EAST search notes	11-27-12	BH

INTERFERENCE SEARCH			
Class	Subclass	Date	Examiner

	/BRANDON HOFFMAN/ Primary Examiner.Art Unit 2433



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
13/585,408	08/14/2012	Mark J. Stefik	10-510-US-C73

CONFIRMATION NO. 4941

PUBLICATION NOTICE



OC000000058145339

98804
Reed Smith LLP
P.O. Box 488
Pittsburgh, PA 15230

Title:SYSTEM AND METHOD FOR DISTRIBUTING DIGITAL CONTENT TO BE RENDERED IN ACCORDANCE WITH USAGE RIGHTS INFORMATION

Publication No.US-2012-0317658-A1

Publication Date:12/13/2012

NOTICE OF PUBLICATION OF APPLICATION

The above-identified application will be electronically published as a patent application publication pursuant to 37 CFR 1.211, et seq. The patent application publication number and publication date are set forth above.

The publication may be accessed through the USPTO's publically available Searchable Databases via the Internet at www.uspto.gov. The direct link to access the publication is currently <http://www.uspto.gov/patft/>.

The publication process established by the Office does not provide for mailing a copy of the publication to applicant. A copy of the publication may be obtained from the Office upon payment of the appropriate fee set forth in 37 CFR 1.19(a)(1). Orders for copies of patent application publications are handled by the USPTO's Office of Public Records. The Office of Public Records can be reached by telephone at (703) 308-9726 or (800) 972-6382, by facsimile at (703) 305-8759, by mail addressed to the United States Patent and Trademark Office, Office of Public Records, Alexandria, VA 22313-1450 or via the Internet.

In addition, information on the status of the application, including the mailing date of Office actions and the dates of receipt of correspondence filed in the Office, may also be accessed via the Internet through the Patent Electronic Business Center at www.uspto.gov using the public side of the Patent Application Information and Retrieval (PAIR) system. The direct link to access this status information is currently <http://pair.uspto.gov/>. Prior to publication, such status information is confidential and may only be obtained by applicant using the private side of PAIR.

Further assistance in electronically accessing the publication, or about PAIR, is available by calling the Patent Electronic Business Center at 1-866-217-9197.

Office of Data Management, Application Assistance Unit (571) 272-4000, or (571) 272-4200, or 1-888-786-0101

Doc Code: DIST.E.FILE Document Description: Electronic Terminal Disclaimer - Filed		PTO/SB/25 U.S. Patent and Trademark Office Department of Commerce	
Electronic Petition Request	TERMINAL DISCLAIMER TO OBIATE A PROVISIONAL DOUBLE PATENTING REJECTION OVER A PENDING "REFERENCE" APPLICATION		
Application Number	13585408		
Filing Date	14-Aug-2012		
First Named Inventor	Mark Stefik		
Attorney Docket Number	10-510-US-C73		
Title of Invention	SYSTEM AND METHOD FOR DISTRIBUTING DIGITAL CONTENT TO BE RENDERED IN ACCORDANCE WITH USAGE RIGHTS INFORMATION		
☒ Filing of terminal disclaimer does not obviate requirement for response under 37 CFR 1.111 to outstanding Office Action ☒ This electronic Terminal Disclaimer is not being used for a Joint Research Agreement.			
Owner		Percent Interest	
ContentGuard Holdings, Inc.		100%	
The owner(s) of percent interest listed above in the instant application hereby disclaims, except as provided below, the terminal part of the statutory term of any patent granted on the instant application which would extend beyond the expiration date of the full statutory term of any patent granted on pending reference Application Number(s)			
13584782 filed on 08/13/2012 as the term of any patent granted on said reference application may be shortened by any terminal disclaimer filed prior to the grant of any patent on the pending reference application. The owner hereby agrees that any patent so granted on the instant application shall be enforceable only for and during such period that it and any patent granted on the reference application are commonly owned. This agreement runs with any patent granted on the instant application and is binding upon the grantee, its successors or assigns. In making the above disclaimer, the owner does not disclaim the terminal part of any patent granted on the instant application that would extend to the expiration date of the full statutory term of any patent granted on said reference application, "as the term of any patent granted on said reference application may be shortened by any terminal disclaimer filed prior to the grant of any patent on the pending reference application," in the event that any such patent granted on the pending reference application: expires for failure to pay a maintenance fee, is held unenforceable, is found invalid by a court of competent jurisdiction, is statutorily disclaimed in whole or terminally disclaimed under 37 CFR 1.321, has all claims canceled by a reexamination certificate, is reissued, or is in any manner terminated prior to the expiration of its full statutory term as shortened by any terminal disclaimer filed prior to its grant.			
☒ Terminal disclaimer fee under 37 CFR 1.20(d) is included with Electronic Terminal Disclaimer request.			

☐ I certify, in accordance with 37 CFR 1.4(d)(4), that the terminal disclaimer fee under 37 CFR 1.20(d) required for this terminal disclaimer has already been paid in the above-identified application.	
☐ Applicant claims SMALL ENTITY status. See 37 CFR 1.27. ☐ Applicant is no longer claiming SMALL ENTITY status. See 37 CFR 1.27(g)(2). ☐ Applicant(s) status remains as SMALL ENTITY. ☒ Applicant(s) status remains as other than SMALL ENTITY.	
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 patent issued thereon.	
THIS PORTION MUST BE COMPLETED BY THE SIGNATORY OR SIGNATORIES I certify, in accordance with 37 CFR 1.4(d)(4) that I am: ☒ An attorney or agent registered to practice before the Patent and Trademark Office who is of record in this application Registration Number <u>58247</u> ☐ A sole inventor ☐ A joint inventor; I certify that I am authorized to sign this submission on behalf of all of the inventors ☐ A joint inventor; all of whom are signing this request ☐ The assignee of record of the entire interest that has properly made itself of record pursuant to 37 <u>CFR 3.71</u>	
Signature	/Stephen M. Hertzler/
Name	Stephen M. Hertzler

*Statement under 37 CFR 3.73(b) is required if terminal disclaimer is signed by the assignee (owner).
 Form PTO/SB/96 may be used for making this certification. See MPEP § 324.

Electronic Patent Application Fee Transmittal

Application Number:	13585408			
Filing Date:	14-Aug-2012			
Title of Invention:	SYSTEM AND METHOD FOR DISTRIBUTING DIGITAL CONTENT TO BE RENDERED IN ACCORDANCE WITH USAGE RIGHTS INFORMATION			
First Named Inventor/Applicant Name:	Mark J. Stefik			
Filer:	Stephen M. Hertzler			
Attorney Docket Number:	10-510-US-C73			
Filed as Large Entity				
Utility under 35 USC 111(a) Filing Fees				
Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Basic Filing:				
Statutory or terminal disclaimer	1814	1	160	160
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Miscellaneous:				
Total in USD (\$)				160

Doc Code: DISQ.E.FILE

Document Description: Electronic Terminal Disclaimer – Approved

Application No.: 13585408

Filing Date: 14-Aug-2012

Applicant/Patent under Reexamination: Stefik et al.

Electronic Terminal Disclaimer filed on December 17, 2012

☒ APPROVED

This patent is subject to a terminal disclaimer

☐ DISAPPROVED

Approved/Disapproved by: Electronic Terminal Disclaimer automatically approved by EFS-Web

U.S. Patent and Trademark Office

Electronic Acknowledgement Receipt

EFS ID:	14483105
Application Number:	13585408
International Application Number:	
Confirmation Number:	4941
Title of Invention:	SYSTEM AND METHOD FOR DISTRIBUTING DIGITAL CONTENT TO BE RENDERED IN ACCORDANCE WITH USAGE RIGHTS INFORMATION
First Named Inventor/Applicant Name:	Mark J. Stefik
Customer Number:	98804
Filer:	Stephen M. Hertzler
Filer Authorized By:	
Attorney Docket Number:	10-510-US-C73
Receipt Date:	17-DEC-2012
Filing Date:	14-AUG-2012
Time Stamp:	13:05:36
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Credit Card
Payment was successfully received in RAM	\$ 160
RAM confirmation Number	12274
Deposit Account	501529
Authorized User	HERTZLER, STEPHEN M.

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:
Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees)
Charge any Additional Fees required under 37 C.F.R. Section 1.19 (Document supply fees)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Electronic Terminal Disclaimer-Filed	eTerminal-Disclaimer.pdf	34292	no	2
			00982becdb1b8713db35cd8c5cb4998bc28191f4		

Warnings:**Information:**

2	Fee Worksheet (SB06)	fee-info.pdf	30504	no	2
			191379bfd6176b7eb428071ba51226a0fe4e285e		

Warnings:**Information:**

Total Files Size (in bytes):	64796

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.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:	)	Confirmation No. 4941
Mark J. Stefik, et al.	)	Group Art Unit: 2433
Serial No. 13/585,408	)	Examiner: Hoffman, Brandon S
Filed: August 14, 2012	)	
For: SYSTEM AND METHOD FOR	)	Date: December 17, 2012
DISTRIBUTING DIGITAL CONTENT	)	
TO BE RENDERED IN ACCORDANCE	)	
WITH USAGE RIGHTS	)	
INFORMATION	)	

RESPONSE TO FINAL OFFICE ACTION

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

In response to the final Office Action mailed December 4, 2012, Applicants submit the following remarks. Applicants respectfully request reconsideration and allowance of this application.

A **Listing of the Claims** begins on page 2 of this paper.

Remarks begin on page 7 of this paper.

Listing of the Claims:

1. (Original) A computer-implemented method of distributing digital content to at least one recipient computing device to be rendered by the at least one recipient computing device in accordance with usage rights information, the method comprising:

determining, by at least one sending computing device, if the at least one recipient computing device is trusted to receive the digital content from the at least one sending computing device;

sending the digital content, by the at least one sending computing device, to the at least one recipient computing device only if the at least one recipient computing device has been determined to be trusted to receive the digital content from the at least one sending computing device; and

sending usage rights information indicating how the digital content may be rendered by the at least one recipient computing device, the usage rights information being enforceable by the at least one recipient computing device.

2. (Original) The method of claim 1, wherein the usage rights information further includes a condition under which the content can be rendered.

3. (Original) The method of claim 1, wherein the determination of trust comprises:

receiving a request from at least one recipient computing device for an authorization object required to render the digital content; and

transmitting the authorization object to the at least one recipient computing device when it is determined that the request should be granted.

4. (Original) The method of claim 1, wherein the determination of trust comprises:

receiving a registration message from the at least one recipient device, the registration message including an identification certificate of the recipient computing device and a random registration identifier, the identification certificate being certified by a master device;

validating the authenticity of the at least one recipient device;

exchanging messages including at least one session key with the at least one recipient device, the session key to be used in communications; and

conducting a secure transaction using the session key, wherein the secure transaction includes sending the digital content to the at least one recipient device.

5. (Previously Presented) The method of claim 1, wherein the validating comprises:
- verifying the identification certificate of the at least one recipient device;
 - generating a message to test the authenticity of the at least one recipient device, the generated message including a nonce;
 - sending the generated message to the at least one recipient device; and
 - verifying if the at least one recipient device correctly processed the generated message.

6. (Original) A sending apparatus for distributing digital content to at least one recipient computing device to be rendered by the at least one recipient computing device in accordance with usage rights information, the sending apparatus comprising:

- one or more processors; and

- one or more memories operatively coupled to at least one of the one or more processors and having instructions stored thereon that, when executed by at least one of the one or more processors, cause at least one of the one or more processors to:

- determine if the at least one recipient computing device is trusted to receive the digital content from the sending apparatus;

- send the digital content, by the sending apparatus, to the at least one recipient computing device only if the at least one recipient computing device has been determined to be trusted to receive the digital content from the sending apparatus; and

- send usage rights information indicating how the digital content may be rendered by the at least one recipient computing device, the usage rights information being enforceable by the at least on recipient computing device.

7. (Original) The apparatus of claim 6, wherein the usage rights information further includes a condition under which the content can be rendered.

8. (Original) The apparatus of claim 6, wherein the determination of trust comprises:
 - receiving a request from at least one recipient computing device for an authorization object required to render the digital content; and
 - transmitting the authorization object to the at least one recipient computing device when it is determined that the request should be granted.
9. (Original) The apparatus of claim 6, wherein the determination of trust comprises:
 - receiving a registration message from the at least one recipient device, the registration message including an identification certificate of the recipient computing device and a random registration identifier, the identification certificate being certified by a master device;
 - validating the authenticity of the at least one recipient device;
 - exchanging messages including at least one session key with the at least one recipient device, the session key to be used in communications; and
 - conducting a secure transaction using the session key, wherein the secure transaction includes sending the digital content to the at least one recipient device.
10. (Original) The apparatus of claim 9, wherein the validating comprises:
 - verifying the identification certificate of the at least one recipient device;
 - generating a message to test the authenticity of the at least one recipient device, the generated message including a nonce;
 - sending the generated message to the at least one recipient device; and
 - verifying if the at least one recipient device correctly processed the generated message.
11. (Original) At least one non-transitory computer-readable medium storing computer-readable instructions that, when executed by at least one sending computing device, cause the at least one sending computing device to:
 - determine if the at least one recipient computing device is trusted to receive the digital content from the at least one sending computing device;

send the digital content, by the at least one sending computing device, to the at least one recipient computing device only if the at least one recipient computing device has been determined to be trusted to receive the digital content from the at least one sending computing device; and

send usage rights information indicating how the digital content may be rendered by the at least one recipient computing device, the usage rights information being enforceable by the at least on recipient computing device.

12. (Original) The at least one non-transitory computer-readable medium of claim 11, wherein the usage rights information further includes a condition under which the content can be rendered.

13. (Original) The at least one non-transitory computer-readable medium of claim 11, wherein the determination of trust comprises:

receiving a request from at least one recipient computing device for an authorization object required to render the digital content; and

transmitting the authorization object to the at least one recipient computing device when it is determined that the request should be granted.

14. (Original) The at least one non-transitory computer-readable medium of claim 11, wherein the determination of trust comprises:

receiving a registration message from the at least one recipient device, the registration message including an identification certificate of the recipient computing device and a random registration identifier, the identification certificate being certified by a master device;

validating the authenticity of the at least one recipient device;

exchanging messages including at least one session key with the at least one recipient device, the session key to be used in communications; and

conducting a secure transaction using the session key, wherein the secure transaction includes sending the digital content to the at least one recipient device.

15. (Original) The at least one non-transitory computer-readable medium of claim 14, wherein the validating comprises:

- verifying the identification certificate of the at least one recipient device;
- generating a message to test the authenticity of the at least one recipient device, the generated message including a nonce;
- sending the generated message to the at least one recipient device; and
- verifying if the at least one recipient device correctly processed the generated message.

REMARKS

Claims 1-15 are pending in this application. In view of the above amendments and the following remarks, Applicants request reconsideration and allowance of this application.

The sole rejection remaining in this application is a provisional nonstatutory obviousness-type double patenting rejection over claims 1-18 of U.S. Appl. No. 13/584,782. As the '782 application, which is the earlier filed application, has been allowed, Applicants submit herewith a Terminal Disclaimer over the '782 application. Thus, this provisional rejection is overcome and should be withdrawn.

In view of the foregoing, Applicants submit that this application is in condition for immediate allowance. If necessary, the Commissioner is hereby authorized to charge fees and credit overpayments to Deposit Account No. 50-1529. If any further information is needed, please contact the undersigned.

Date: December 17, 2012

Respectfully submitted,
/Stephen M. Hertzler, Reg. No. 58,247/
Stephen M. Hertzler
Registration No. 58,247

REED SMITH LLP
CUSTOMER NO.: 98804
1301 K Street N.W.
Suite 1100 – East Tower
Washington, D.C. 20005

Electronic Acknowledgement Receipt

EFS ID:	14483154
Application Number:	13585408
International Application Number:	
Confirmation Number:	4941
Title of Invention:	SYSTEM AND METHOD FOR DISTRIBUTING DIGITAL CONTENT TO BE RENDERED IN ACCORDANCE WITH USAGE RIGHTS INFORMATION
First Named Inventor/Applicant Name:	Mark J. Stefik
Customer Number:	98804
Filer:	Stephen M. Hertzler
Filer Authorized By:	
Attorney Docket Number:	10-510-US-C73
Receipt Date:	17-DEC-2012
Filing Date:	14-AUG-2012
Time Stamp:	13:08:44
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		10-510-US-C73_-_2012-12-17_-_Response.pdf	490699 609e8c3705fd5965f4a145dc25268b406fb7285c	yes	7

	Multipart Description/PDF files in .zip description		
	Document Description	Start	End
	Amendment After Final	1	1
	Claims	2	6
	Applicant Arguments/Remarks Made in an Amendment	7	7
Warnings:			
Information:			
Total Files Size (in bytes):		490699	
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. <u>New Applications Under 35 U.S.C. 111</u> 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. <u>National Stage of an International Application under 35 U.S.C. 371</u> 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. <u>New International Application Filed with the USPTO as a Receiving Office</u> 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.			

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.

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875					Application or Docket Number 13/585,408		Filing Date 08/14/2012		☐ To be Mailed			
APPLICATION AS FILED – PART I												
(Column 1)			(Column 2)		SMALL ENTITY ☐		OR		OTHER THAN SMALL ENTITY			
FOR	NUMBER FILED	NUMBER EXTRA	RATE (\$)	FEE (\$)	RATE (\$)	FEE (\$)						
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A		N/A							
☐ SEARCH FEE (37 CFR 1.16(k), (l), or (m))	N/A	N/A	N/A		N/A							
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A		N/A							
TOTAL CLAIMS (37 CFR 1.16(j))	minus 20 =	*	X \$	=	X \$	=						
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*	X \$	=	X \$	=						
☐ APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is \$250 (\$125 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).											
☐ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))												
* If the difference in column 1 is less than zero, enter "0" in column 2.												
APPLICATION AS AMENDED – PART II												
(Column 1)			(Column 2)		(Column 3)		SMALL ENTITY		OR		OTHER THAN SMALL ENTITY	
AMENDMENT	12/17/2012	CLAIMS REMAINING AFTER AMENDMENT	HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE (\$)	ADDITIONAL FEE (\$)	RATE (\$)	ADDITIONAL FEE (\$)				
	Total (37 CFR 1.16(i))	* 15	Minus	** 20	= 0	X \$	=	X \$62=	0			
	Independent (37 CFR 1.16(h))	* 3	Minus	***3	= 0	X \$	=	X \$250=	0			
	☐ Application Size Fee (37 CFR 1.16(s))											
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))											
					TOTAL ADD'L FEE		TOTAL ADD'L FEE	0				
(Column 1)			(Column 2)		(Column 3)		SMALL ENTITY		OR		OTHER THAN SMALL ENTITY	
AMENDMENT	CLAIMS REMAINING AFTER AMENDMENT	HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE (\$)	ADDITIONAL FEE (\$)	RATE (\$)	ADDITIONAL FEE (\$)					
	Total (37 CFR 1.16(i))	*	Minus	**	=	X \$	=	X \$	=			
	Independent (37 CFR 1.16(h))	*	Minus	***	=	X \$	=	X \$	=			
	☐ Application Size Fee (37 CFR 1.16(s))											
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))											
					TOTAL ADD'L FEE		TOTAL ADD'L FEE					
* If the entry in column 1 is less than the entry in column 2, write "0" in column 3. ** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20". *** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3". The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.												

Legal Instrument Examiner:
/BRENDA J. DENNY/

This collection of information is required by 37 CFR 1.16. 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 1.14. 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.**

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



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

NOTICE OF ALLOWANCE AND FEE(S) DUE

98804 7590 01/11/2013
Reed Smith LLP
P.O. Box 488
Pittsburgh, PA 15230

EXAMINER

HOFFMAN, BRANDON S

ART UNIT

PAPER NUMBER

2433

DATE MAILED: 01/11/2013

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.

13/585,408

08/14/2012

Mark J. Stefik

10-510-US-C73

4941

TITLE OF INVENTION: SYSTEM AND METHOD FOR DISTRIBUTING DIGITAL CONTENT TO BE RENDERED IN ACCORDANCE WITH USAGE RIGHTS INFORMATION

APPLN. TYPE	SMALL ENTITY	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	NO	\$1770	\$0	\$0	\$1770	04/11/2013

THE APPLICATION IDENTIFIED ABOVE HAS BEEN EXAMINED AND IS ALLOWED FOR ISSUANCE AS A PATENT. PROSECUTION ON THE MERITS IS CLOSED. THIS NOTICE OF ALLOWANCE IS NOT A GRANT OF PATENT RIGHTS. THIS APPLICATION IS SUBJECT TO WITHDRAWAL FROM ISSUE AT THE INITIATIVE OF THE OFFICE OR UPON PETITION BY THE APPLICANT. SEE 37 CFR 1.313 AND MPEP 1308.

THE ISSUE FEE AND PUBLICATION FEE (IF REQUIRED) MUST BE PAID WITHIN THREE MONTHS FROM THE MAILING DATE OF THIS NOTICE OR THIS APPLICATION SHALL BE REGARDED AS ABANDONED. THIS STATUTORY PERIOD CANNOT BE EXTENDED. SEE 35 U.S.C. 151. THE ISSUE FEE DUE INDICATED ABOVE DOES NOT REFLECT A CREDIT FOR ANY PREVIOUSLY PAID ISSUE FEE IN THIS APPLICATION. IF AN ISSUE FEE HAS PREVIOUSLY BEEN PAID IN THIS APPLICATION (AS SHOWN ABOVE), THE RETURN OF PART B OF THIS FORM WILL BE CONSIDERED A REQUEST TO REAPPLY THE PREVIOUSLY PAID ISSUE FEE TOWARD THE ISSUE FEE NOW DUE.

HOW TO REPLY TO THIS NOTICE:

I. Review the SMALL ENTITY status shown above.

If the SMALL ENTITY is shown as YES, verify your current SMALL ENTITY status:

A. If the status is the same, pay the TOTAL FEE(S) DUE shown above.

B. If the status above is to be removed, check box 5b on Part B - Fee(s) Transmittal and pay the PUBLICATION FEE (if required) and twice the amount of the ISSUE FEE shown above, or

If the SMALL ENTITY is shown as NO:

A. Pay TOTAL FEE(S) DUE shown above, or

B. If applicant claimed SMALL ENTITY status before, or is now claiming SMALL ENTITY status, check box 5a on Part B - Fee(s) Transmittal and pay the PUBLICATION FEE (if required) and 1/2 the ISSUE FEE shown above.

II. PART B - FEE(S) TRANSMITTAL, or its equivalent, must be completed and returned to the United States Patent and Trademark Office (USPTO) with your ISSUE FEE and PUBLICATION FEE (if required). If you are charging the fee(s) to your deposit account, section "4b" of Part B - Fee(s) Transmittal should be completed and an extra copy of the form should be submitted. If an equivalent of Part B is filed, a request to reapply a previously paid issue fee must be clearly made, and delays in processing may occur due to the difficulty in recognizing the paper as an equivalent of Part B.

III. All communications regarding this application must give the application number. Please direct all communications prior to issuance to Mail Stop ISSUE FEE unless advised to the contrary.

IMPORTANT REMINDER: Utility patents issuing on applications filed on or after Dec. 12, 1980 may require payment of maintenance fees. It is patentee's responsibility to ensure timely payment of maintenance fees when due.

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), to: **Mail** Mail Stop ISSUE FEE
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450
or Fax (571)-273-2885

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

98804 7590 01/11/2013
Reed Smith LLP
P.O. Box 488
Pittsburgh, PA 15230

Certificate of Mailing or Transmission

I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being facsimile transmitted to the USPTO (571) 273-2885, on the date indicated below.

(Depositor's name)
(Signature)
(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.

13/585,408 08/14/2012 Mark J. Stefik 10-510-US-C73 4941

TITLE OF INVENTION: SYSTEM AND METHOD FOR DISTRIBUTING DIGITAL CONTENT TO BE RENDERED IN ACCORDANCE WITH USAGE RIGHTS INFORMATION

APPLN. TYPE	SMALL ENTITY	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	NO	\$1770	\$0	\$0	\$1770	04/11/2013

EXAMINER	ART UNIT	CLASS-SUBCLASS
HOFFMAN, BRANDON S	2433	726-029000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).

- ☐ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.
☐ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-02 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list

- (1) the names of up to 3 registered patent attorneys or agents OR, alternatively, 1 _____
(2) the name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed. 2 _____
3 _____

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document has been filed for recordation as set forth in 37 CFR 3.11. Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE (B) RESIDENCE: (CITY and STATE OR COUNTRY)

Please check the appropriate assignee category or categories (will not be printed on the patent): ☐ Individual ☐ Corporation or other private group entity ☐ Government

4a. The following fee(s) are submitted:

- ☐ Issue Fee
☐ Publication Fee (No small entity discount permitted)
☐ Advance Order - # of Copies _____

4b. Payment of Fee(s); (Please first reapply any previously paid issue fee shown above)

- ☐ A check is enclosed.
☐ Payment by credit card. Form PTO-2038 is attached.
☐ The Director is hereby authorized to charge the required fee(s), any deficiency, or credit any overpayment, to Deposit Account Number _____ (enclose an extra copy of this form).

5. Change in Entity Status (from status indicated above)

- ☐ a. Applicant claims SMALL ENTITY status. See 37 CFR 1.27. ☐ b. Applicant is no longer claiming SMALL ENTITY status. See 37 CFR 1.27(g)(2).

NOTE: The Issue Fee and Publication Fee (if required) will not be accepted from anyone other than the applicant; a registered attorney or agent; or the assignee or other party in interest as shown by the records of the United States Patent and Trademark Office.

Authorized Signature _____ Date _____

Typed or printed name _____ Registration No. _____

This collection of information is required by 37 CFR 1.311. 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 1.14. 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, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450.

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.



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/585,408	08/14/2012	Mark J. Stefik	10-510-US-C73	4941
98804	7590	01/11/2013	EXAMINER	
Reed Smith LLP P.O. Box 488 Pittsburgh, PA 15230			HOFFMAN, BRANDON S	
			ART UNIT	PAPER NUMBER
			2433	
DATE MAILED: 01/11/2013				

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b) (application filed on or after May 29, 2000)

The Patent Term Adjustment to date is 0 day(s). If the issue fee is paid on the date that is three months after the mailing date of this notice and the patent issues on the Tuesday before the date that is 28 weeks (six and a half months) after the mailing date of this notice, the Patent Term Adjustment will be 0 day(s).

If a Continued Prosecution Application (CPA) was filed in the above-identified application, the filing date that determines Patent Term Adjustment is the filing date of the most recent CPA.

Applicant will be able to obtain more detailed information by accessing the Patent Application Information Retrieval (PAIR) WEB site (<http://pair.uspto.gov>).

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Customer Service Center of the Office of Patent Publication at 1-(888)-786-0101 or (571)-272-4200.

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Notice of Allowability	Application No.	Applicant(s)	
	13/585,408	STEFIK ET AL.	
	Examiner	Art Unit	
	BRANDON HOFFMAN	2433	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to amendment filed December 17, 2012.
2. ☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on ____; the restriction requirement and election have been incorporated into this action.
3. ☒ The allowed claim(s) is/are 1-15. As a result of the allowed claim(s), you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to PPHfeedback@uspto.gov.
4. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
 - a) ☐ All b) ☐ Some* c) ☐ None of the:
 1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. ____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

* Certified copies not received: ____.

Applicant has **THREE MONTHS FROM THE "MAILING DATE"** of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.

THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.

☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).
6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892) 2. ☐ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date _____ 3. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material 4. ☐ Interview Summary (PTO-413), Paper No./Mail Date _____	5. ☐ Examiner's Amendment/Comment 6. ☐ Examiner's Statement of Reasons for Allowance 7. ☐ Other _____

/Brandon S Hoffman/
Primary Examiner, Art Unit 2433

<i>Index of Claims</i> 	Application/Control No. 13585408	Applicant(s)/Patent Under Reexamination STEFIK ET AL.
	Examiner BRANDON HOFFMAN	Art Unit 2433

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☒ Claims renumbered in the same order as presented by applicant					☐ CPA		☒ T.D.		☐ R.1.47	
CLAIM		DATE								
Final	Original	10/09/2012	11/27/2012	01/01/2013						
	1	✓	✓	=						
	2	✓	✓	=						
	3	✓	✓	=						
	4	✓	✓	=						
	5	✓	✓	=						
	6	✓	✓	=						
	7	✓	✓	=						
	8	✓	✓	=						
	9	✓	✓	=						
	10	✓	✓	=						
	11	✓	✓	=						
	12	✓	✓	=						
	13	✓	✓	=						
	14	✓	✓	=						
	15	✓	✓	=						

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:	)	Confirmation No. 4941
Mark J. Stefik, et al.	)	Group Art Unit: 2433
Serial No. 13/585,408	)	Examiner: Hoffman, Brandon S
Filed: August 14, 2012	)	
For: SYSTEM AND METHOD FOR	)	Date: December 17, 2012
DISTRIBUTING DIGITAL CONTENT	)	
TO BE RENDERED IN ACCORDANCE	)	
WITH USAGE RIGHTS	)	
INFORMATION	)	

RESPONSE TO FINAL OFFICE ACTION

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

In response to the final Office Action mailed December 4, 2012, Applicants submit the following remarks. Applicants respectfully request reconsideration and allowance of this application.

A Listing of the Claims begins on page 2 of this paper.

Remarks begin on page 7 of this paper.

OK TO ENTER: /BH/

Search Notes 	Application/Control No. 13585408	Applicant(s)/Patent Under Reexamination STEFIK ET AL.
	Examiner BRANDON HOFFMAN	Art Unit 2433

SEARCHED			
Class	Subclass	Date	Examiner
726	29 - with keyword limiters	10-9-12	BH

SEARCH NOTES		
Search Notes	Date	Examiner
inventor name search	10-9-12	BH
see attached EAST search notes	10-9-12	BH
updated EAST search notes	11-27-12	BH
updated EAST search notes	1-1-13	BH

INTERFERENCE SEARCH			
Class	Subclass	Date	Examiner
	searched claim language	1-1-13	BH

	/BRANDON HOFFMAN/ Primary Examiner.Art Unit 2433

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	1040792	recipient receiver	US-PGPUB; USPAT; USOCR	OR	OFF	2013/01/01 10:33
L2	663508	sender sending	US-PGPUB; USPAT; USOCR	OR	OFF	2013/01/01 10:33
L3	105343	trust\$3	US-PGPUB; USPAT; USOCR	OR	OFF	2013/01/01 10:33
L4	1342915	render\$3	US-PGPUB; USPAT; USOCR	OR	OFF	2013/01/01 10:34
L5	4393	usage with rights	US-PGPUB; USPAT; USOCR	OR	OFF	2013/01/01 10:34
L6	701	1 and 2 and 3 and 4 and 5	US-PGPUB; USPAT; USOCR	OR	OFF	2013/01/01 10:34
L7	0	6 and @ad<"19941123"	US-PGPUB; USPAT; USOCR	OR	OFF	2013/01/01 10:34
L8	10954	3.clm.	US-PGPUB; USPAT; USOCR	OR	OFF	2013/01/01 10:34
L9	96780	4.clm.	US-PGPUB; USPAT; USOCR	OR	OFF	2013/01/01 10:34
L10	799	5.clm.	US-PGPUB; USPAT; USOCR	OR	OFF	2013/01/01 10:34
L11	33	8 and 9 and 10	US-PGPUB; USPAT; USOCR	OR	OFF	2013/01/01 10:34
S1	1227	(726/29).CCLS.	US-PGPUB; USPAT; USOCR	OR	OFF	2012/10/09 13:48
S2	209	(STEFIK near MARK PIROLI near PETER).in.	US-PGPUB; USPAT; USOCR	OR	OFF	2012/10/09 13:49
S3	4	("4817140" "5204961" "5390297" "6135646").PN.	US-PGPUB; USPAT; USOCR	OR	OFF	2012/10/09 13:50
S4	102095	trust\$3	US-PGPUB; USPAT; USOCR	OR	OFF	2012/10/09 13:51
S5	2359	usage adj rights	US-PGPUB; USPAT; USOCR	OR	OFF	2012/10/09 14:04
S6	249736	authentic\$5	US-PGPUB; USPAT; USOCR	OR	OFF	2012/10/09 14:05
S7	1324520	render\$3	US-PGPUB; USPAT; USOCR	OR	OFF	2012/10/09 14:14
S8	760	S4 and S5 and S6 and S7	US-PGPUB; USPAT; USOCR	OR	OFF	2012/10/09 14:35
S9	34	S1 and S8	US-PGPUB; USPAT; USOCR	OR	OFF	2012/10/09 14:36
S10	113	S2 and S8	US-PGPUB; USPAT; USOCR	OR	OFF	2012/10/09 14:36
S11	0	S9 and @ad<"19941123"	US-PGPUB; USPAT; USOCR	OR	OFF	2012/10/09 15:18

S12	0	S8 and @ad<"19941123"	US-PGPUB; USPAT; USOCR	OR	OFF	2012/10/09 15:18
S13	5	S8 and @ad<"19951123"	US-PGPUB; USPAT; USOCR	OR	OFF	2012/10/09 15:35
S14	1	("6898576").PN.	US-PGPUB; USPAT; USOCR	OR	OFF	2012/10/09 16:48
S15	103872	trust\$3	US-PGPUB; USPAT; USOCR	OR	OFF	2012/11/27 16:44
S16	655828	sender sending	US-PGPUB; USPAT; USOCR	OR	OFF	2012/11/27 16:44
S17	1031087	recipient receiver	US-PGPUB; USPAT; USOCR	OR	OFF	2012/11/27 16:44
S18	4326	usage with rights	US-PGPUB; USPAT; USOCR	OR	OFF	2012/11/27 16:44
S19	1338633	render\$	US-PGPUB; USPAT; USOCR	OR	OFF	2012/11/27 16:44
S20	691	S15 and S16 and S17 and S18 and S19	US-PGPUB; USPAT; USOCR	OR	OFF	2012/11/27 16:44
S21	0	S20 and @ad<"19941123"	US-PGPUB; USPAT; USOCR	OR	OFF	2012/11/27 16:45

1/ 1/ 2013 10:35:47 AM
C:\ Users\ bhoffman\ Documents\ EAST\ Workspaces\ 13585408.wsp

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), to: **Mail** **Mail Stop ISSUE FEE**
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450
or Fax (571)-273-2885

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

98804 7590 01/11/2013
Reed Smith LLP
P.O. Box 488
Pittsburgh, PA 15230

Certificate of Mailing or Transmission

I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being facsimile transmitted to the USPTO (571) 273-2885, on the date indicated below.

(Depositor's name)
(Signature)
(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.

13/585,408 08/14/2012 Mark J. Stefik 10-510-US-C73 4941

TITLE OF INVENTION: SYSTEM AND METHOD FOR DISTRIBUTING DIGITAL CONTENT TO BE RENDERED IN ACCORDANCE WITH USAGE RIGHTS INFORMATION

APPLN. TYPE	SMALL ENTITY	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	NO	\$1770	\$0	\$0	\$1770	04/11/2013

EXAMINER	ART UNIT	CLASS-SUBCLASS
HOFFMAN, BRANDON S	2433	726-029000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).

☐ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.

☐ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-02 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list

(1) the names of up to 3 registered patent attorneys or agents OR, alternatively,

(2) the name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.

1 Marc S. Kaufman

2 Stephen M. Hertzler

3 Reed Smith LLP

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document has been filed for recordation as set forth in 37 CFR 3.11. Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE

(B) RESIDENCE: (CITY and STATE OR COUNTRY)

ContentGuard Holdings, Inc.

Wilmington, DE

Please check the appropriate assignee category or categories (will not be printed on the patent): ☐ Individual ☒ Corporation or other private group entity ☐ Government

4a. The following fee(s) are submitted:

☒ Issue Fee

☐ Publication Fee (No small entity discount permitted)

☐ Advance Order - # of Copies _____

4b. Payment of Fee(s); (Please first reapply any previously paid issue fee shown above)

☐ A check is enclosed.

☐ Payment by credit card. Form PTO-2038 is attached.

☒ The Director is hereby authorized to charge the required fee(s), any deficiency, or credit any overpayment, to Deposit Account Number 50-1529 (enclose an extra copy of this form).

5. Change in Entity Status (from status indicated above)

☐ a. Applicant claims SMALL ENTITY status. See 37 CFR 1.27.

☐ b. Applicant is no longer claiming SMALL ENTITY status. See 37 CFR 1.27(g)(2).

NOTE: The Issue Fee and Publication Fee (if required) will not be accepted from anyone other than the applicant; a registered attorney or agent; or the assignee or other party in interest as shown by the records of the United States Patent and Trademark Office.

Authorized Signature /Marc S. Kaufman, Reg. No. 35,212/

Date January 30, 2013

Typed or printed name Marc S. Kaufman

Registration No. 35,212

This collection of information is required by 37 CFR 1.311. 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 1.14. 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, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450.

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.

Electronic Patent Application Fee Transmittal

Application Number:	13585408			
Filing Date:	14-Aug-2012			
Title of Invention:	SYSTEM AND METHOD FOR DISTRIBUTING DIGITAL CONTENT TO BE RENDERED IN ACCORDANCE WITH USAGE RIGHTS INFORMATION			
First Named Inventor/Applicant Name:	Mark J. Stefik			
Filer:	Marc S. Kaufman			
Attorney Docket Number:	10-510-US-C73			
Filed as Large Entity				
Utility under 35 USC 111(a) Filing Fees				
Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Utility Appl issue fee	1501	1	1770	1770
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Miscellaneous:				
Total in USD (\$)				1770

Electronic Acknowledgement Receipt

EFS ID:	14826207
Application Number:	13585408
International Application Number:	
Confirmation Number:	4941
Title of Invention:	SYSTEM AND METHOD FOR DISTRIBUTING DIGITAL CONTENT TO BE RENDERED IN ACCORDANCE WITH USAGE RIGHTS INFORMATION
First Named Inventor/Applicant Name:	Mark J. Stefik
Customer Number:	98804
Filer:	Marc S. Kaufman/Stephen Hertzler
Filer Authorized By:	Marc S. Kaufman
Attorney Docket Number:	10-510-US-C73
Receipt Date:	30-JAN-2013
Filing Date:	14-AUG-2012
Time Stamp:	21:11:49
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Credit Card
Payment was successfully received in RAM	\$1770
RAM confirmation Number	10415
Deposit Account	501529
Authorized User	HERTZLER, STEPHEN M.

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.19 (Document supply fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.20 (Post Issuance fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.21 (Miscellaneous fees and charges)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Issue Fee Payment (PTO-85B)	10-510-US-C73_-_2013-01-30_-_Issue_Fee_Payment.pdf	2142008	no	1
			d610963f4dc1c4989f4b286474c35e678ed d9bd7		

Warnings:

Information:

2	Fee Worksheet (SB06)	fee-info.pdf	30190	no	2
			7a7cc3297e985ef9dd44952b4aee4758276 29451		

Warnings:

Information:

Total Files Size (in bytes):			2172198

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.



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	ISSUE DATE	PATENT NO.	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/585,408	03/05/2013	8393007	10-510-US-C73	4941

98804 7590 02/13/2013
Reed Smith LLP
P.O. Box 488
Pittsburgh, PA 15230

ISSUE NOTIFICATION

The projected patent number and issue date are specified above.

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b) (application filed on or after May 29, 2000)

The Patent Term Adjustment is 0 day(s). Any patent to issue from the above-identified application will include an indication of the adjustment on the front page.

If a Continued Prosecution Application (CPA) was filed in the above-identified application, the filing date that determines Patent Term Adjustment is the filing date of the most recent CPA.

Applicant will be able to obtain more detailed information by accessing the Patent Application Information Retrieval (PAIR) WEB site (<http://pair.uspto.gov>).

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Application Assistance Unit (AAU) of the Office of Data Management (ODM) at (571)-272-4200.

APPLICANT(s) (Please see PAIR WEB site <http://pair.uspto.gov> for additional applicants):

Mark J. Stefik, Portola Valley, CA;
Peter L.T. Pirolli, San Francisco, CA;

The United States represents the largest, most dynamic marketplace in the world and is an unparalleled location for business investment, innovation, and commercialization of new technologies. The USA offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to encourage and facilitate business investment. To learn more about why the USA is the best country in the world to develop technology, manufacture products, and grow your business, visit SelectUSA.gov.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		13585408
	Filing Date		2012-08-14
	First Named Inventor	Mark J. STEFIK	
	Art Unit	2433	
	Examiner Name	BRANDON S HOFFMAN	
	Attorney Docket Number	10-510-US-C73	

U.S.PATENTS						Remove
Examiner Initial*	Cite No	Patent Number	Kind Code ¹	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	5406628		1995-04-11	Beller et al.	
	2	4868877		1989-09-19	Fischer, Addison M.	
	3	5553139		1996-09-03	Ross et al.	
	4	5586186		1996-12-17	Yuval et al.	
	5	5936149		1999-08-10	Fischer, Addison M.	
	6	5288978		1994-02-22	Iijima, Yasuo	
	7	5345506		1994-09-06	Tsubakuyama et al.	
	8	5619657		1997-04-08	Sudama et al.	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number		13585408
Filing Date		2012-08-14
First Named Inventor	Mark J. STEFIK	
Art Unit	2433	
Examiner Name	BRANDON S HOFFMAN	
Attorney Docket Number	10-510-US-C73	

9	5375206		1994-12-20	Hunter et al.	
10	5287434		1994-02-15	Bain et al.	
11	5940504		1999-08-17	Griswold, Gary N.	
12	6135646		2000-10-24	Kahn et al.	
13	5715403		1998-02-03	Stefik, Mark J.	
14	5629980		1997-05-13	Stefik et al.	
15	5260999		1993-11-09	Wyman, Robert M.	
16	5146575		1992-09-08	Thomas J. Nolan, Jr.	
17	5412717		1995-05-02	Addison M. Fischer	
18	5390247		1995-02-14	Addison M. Fischer	
19	5444779		1995-08-22	Daniele	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		13585408	
	Filing Date		2012-08-14	
	First Named Inventor	Mark J. STEFIK		
	Art Unit	2433		
	Examiner Name	BRANDON S HOFFMAN		
	Attorney Docket Number	10-510-US-C73		

	20	5920861		1999-07-06	Hall	
	21	5986690		1999-11-16	Hendricks	
	22	5588146		1996-12-24	Leroux	
	23	4868736		1989-09-19	Walker	

If you wish to add additional U.S. Patent citation information please click the Add button. [Add](#)

U.S.PATENT APPLICATION PUBLICATIONS							Remove

Examiner Initial*	Cite No	Publication Number	Kind Code ¹	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20030046093		2003-03-06	Erickson, et al.	
	2	20020157002		2002-10-24	Messerges, et al.	
	3	20030126086		2003-07-03	Safadi	

If you wish to add additional U.S. Published Application citation information please click the Add button. [Add](#)

FOREIGN PATENT DOCUMENTS								Remove

Examiner Initial*	Cite No	Foreign Document Number ³	Country Code ²	Kind Code ⁴	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T ⁵

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		13585408	
	Filing Date		2012-08-14	
	First Named Inventor	Mark J. STEFIK		
	Art Unit	2433		
	Examiner Name	BRANDON S HOFFMAN		
	Attorney Docket Number	10-510-US-C73		

	1	0268139	EP	A2	1988-05-25	Comerford		☐
	2	0464306	EP	A2	1992-01-08	Hartrick		☐
	3	0567800	EP	A1	1993-03-11	Hartrick		☐

If you wish to add additional Foreign Patent Document citation information please click the Add button **Add**

NON-PATENT LITERATURE DOCUMENTS				Remove
Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T ⁵	
	1		☐	

If you wish to add additional non-patent literature document citation information please click the Add button **Add**

EXAMINER SIGNATURE			
Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

¹ See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. ² Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). ³ For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. ⁴ Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. ⁵ Applicant is to place a check mark here if English language translation is attached.

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	13585408
Filing Date	2012-08-14
First Named Inventor	Mark J. STEFIK
Art Unit	2433
Examiner Name	BRANDON S HOFFMAN
Attorney Docket Number	10-510-US-C73

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

☐ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

☐ See attached certification statement.

☒ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Stephen M. Hertzler, Reg. No. 58,247/	Date (YYYY-MM-DD)	2013-02-26
Name/Print	Stephen M. Hertzler	Registration Number	58247

This collection of information is required by 37 CFR 1.97 and 1.98. 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 1.14. This collection is estimated to take 1 hour 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.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these records.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

12 **EUROPEAN PATENT APPLICATION**

21 Application number: **87116179.0**

51 Int. Cl.4: **G06F 1/00**

22 Date of filing: **03.11.87**

30 Priority: **05.11.86 US 927299**

43 Date of publication of application:
25.05.88 Bulletin 88/21

64 Designated Contracting States:
DE FR GB IT

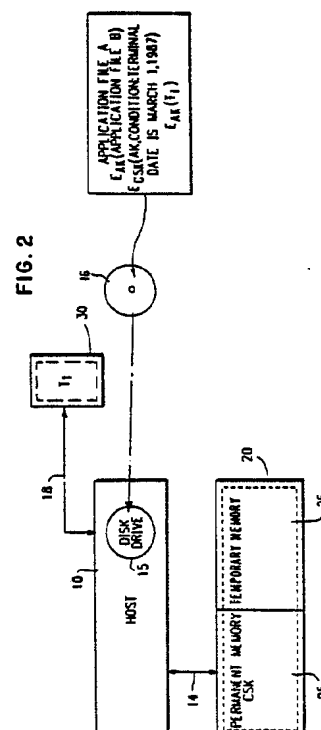
71 Applicant: **International Business Machines Corporation**
Old Orchard Road
Armonk, N.Y. 10504(US)

72 Inventor: **Comerford, Liam David**
Box 191 Rd. No. 1 10 Valley Road
Carmel, N.Y. 10512(US)
Inventor: **White, Steve Richard**
7 Park Avenue Apt. 33
New York, N.Y. 10016(US)

74 Representative: **Teufel, Fritz, Dipl.-Phys. et al**
IBM Deutschland GmbH. Europäische
Patentdienste Postfach 265
D-8000 München 22(DE)

54 **Manipulating rights-to-execute in connection with a software copy protection mechanism.**

57 A software asset protection mechanism segregates the right to execute software from the software itself. The rights to execute, when installed on a composite computing system, (10,20) are stored in a coprocessor element (20) of the composite computing system. The software asset protection mechanism is enhanced as described herein by providing for the manipulation of those rights to execute. More particularly, the rights to execute can be conditioned at least in terms of a valid period of execution or a valid number of executions. The rights to execute can be safely transferred from one coprocessor to another, or can be returned to the software vendor. Finally, a method of backing up the rights to execute to provide the user with the rights to execute in case the coprocessor element of the composite computing system fails.



EP 0 268 139 A2

MANIPULATING RIGHTS-TO-EXECUTE IN CONNECTION WITH A SOFTWARE COPY PROTECTION MECHANISM

Technical Field

The invention is in the field of data processing, especially in connection with a software copy protection mechanism. That mechanism restricts software, distributed on a magnetic disk or other medium, for use on any computer which is associated with an authorized, physically secure coprocessor where the mechanism does not interfere with the user creation of "backup" copies; but the protection is not compromised by any such "backup" copies. The present invention is particularly directed at manipulating a right-to-execute which is a distinguishing characteristic of that copy protection mechanism.

Background of the Invention

The basic copy protection mechanism is described in copending application [YO985-091]; this mechanism separates the software which is to be protected from the right to execute that software. To provide security and implement the mechanism, each computer on which a protected application is to run (hereinafter referred to as a host) is associated with a logically and physically secure coprocessor. When installed in the coprocessor, the right-to-execute a particular protected application exists in the form of a software decryption key called an application key (AK). So long as the software decryption key AK is retained in the permanent memory of the coprocessor, the corresponding protected software can be executed on the composite system including the host and coprocessor. The software copy protection mechanism has the advantage that it negligibly interferes with present and contemplated software distribution techniques, it allows the user to make unlimited numbers of "backup" copies and it does not require any two-way communication between the user and the software vendor. This is supported by distribution of an authorization to the coprocessor to accept a right to execute provided in the form of a hardware cartridge (or token). Furthermore, the user need only employ the token the first time the protected application is run in order to transfer the right to execute, which is represented by the unused token, to the coprocessor. Thereafter, the token may be discarded and it is thereafter totally unnecessary to maintenance or use of the right to execute.

The invention described in copending applica-

tion [YO985-091] does not address manipulation of the right to execute (other than describing how a user may first acquire it), nor does it describe the possibility of conditioning the right to execute. The present invention is particularly directed at conditioning or manipulating or transferring the right to execute which exists in a coprocessor.

In particular, the present invention provides the capability of safely transferring the right to execute. The right to execute may be transferred to another coprocessor or may be merely transferred outside the coprocessor for external storage. In either event it is essential that the process of transferring the right to execute not generate or allow spurious or duplicate rights to execute which would of course defeat the purpose of the copy protection mechanism. As described herein, the transfer of a right to execute can be indirect, through the use of a transfer set (which in many respects is identical to the distribution set through which the right to execute was acquired) or direct via a coprocessor to coprocessor communication link. Safety is maintained even though the communication is unsecured in the sense that the transfer transaction may be observed.

The present invention also provides techniques for conditioning the right to execute. For example, the right to execute might be conditioned by a time period (a right to execute which exists up until a cut-off date and/or time) or it could be conditioned based on the number of times it is invoked (for example the vendor could sell a user the right to execute the protected application ten times). As will be described, the right to execute can be conditioned on any other parameter so long as it can be measured by the coprocessor to the satisfaction of the source of that right to execute (the software vendor). The availability of conditioned rights to execute provides the software vendor with additional flexibility and it further opens up the possibility, for the first time in the software field, of a truly safe "return" policy. For obvious reasons, a software vendor, using today's software distribution techniques, will be in jeopardy of giving his products away free if he accepts the "return" of software for full purchase credit. The vendor has no way of verifying with present distribution techniques whether or not the user has already duplicated the software so that after the return the user could still maintain a fully usable copy of the application. Using the principles described herein, however, the software vendor can implement a "return" policy and be assured that if a user returns the software, the user no longer retains an

executable copy.

Because the software copy protection mechanism operates in the real world, with real world devices, and because the distinct right to execute exists in the form of a cryptographic key stored in the permanent memory of a coprocessor, it is necessary to address the possibility that the coprocessor storing the right to execute may fail. Such failure should not result in the complete loss of the user's rights to execute, and the present invention provides apparatus and methods for securing the user against the loss of the right to execute in the event his coprocessor does fail. Much as in the case with moving or transferring the right to execute, any hardware "backup" technique (available in case a coprocessor fails) should not have the property of being useful to generate spurious rights to execute. The hardware backup method provides minimal opportunity (and significant disincentive) for improperly multiplying rights to execute.

Summary of the Invention

The invention meets these and other objects as described below.

Conditioned Right-to-Execute

In order to condition the right to execute, in a system such as described in our copending application [YO985-091], there must be:

- 1) a statement of the condition (or conditions) under which the application software may (or may not) be allowed to execute fully, and
- 2) some objective criteria against which the condition or conditions can be measured, and
- 3) a software program which can test the conditions against the criteria and act in a way determined by results of that test.

These objectives must be met in a way which is secure against attempts of the user, or anyone else not specifically authorized by the software vendor to either vary the conditions or the objective criteria under which the conditions are met. In accordance with the invention, the criteria are stated in software, and more particularly, in the protected or encrypted portion of the application software. As is described in our copending application [YO985-091], the only form in which the protected application software is available to the user is in encrypted form; because the user does not have access to the decryption key as a data object, he is unable to modify, or even read the protected software. Thus, incorporating the conditions of the right to execute within the protected software results in securing these conditions against alteration by the user or anyone else unless authorized by the software vendor. In order to save (for testing)

the conditions which are tested against the programmed criteria, we use some storage space in the non volatile memory of the coprocessor; this storage space has already allocated to it the function of storing the decryption key necessary to decrypt the encrypted software. Thus the storage space allocated to a particular protected piece of software is expanded to include the condition which can be measured against the criteria. Because of the non-volatility of the memory, so long as the right to execute is available in the coprocessor, the objective conditions are also available. It should be understood that the coprocessor contains a continuously powered real-time clock within its physically secure boundary so that in the case that criteria involving time are to be used, the time information is available. Because the information is stored in a coprocessor's non-volatile memory, and only the portion of this memory allocated to any particular application can be accessed by that application, the information is secure against any attempt at modification by the user. The application software may modify the conditions stored in its portion of non-volatile memory, but may not change the value of the real-time clock.

For example, the software thus could count the number of times or the total period it had been used by changing numbers kept in this storage and executing only until criteria related to number or total period of executions were no longer met by the stored conditions.

As an example, assume that the software vendor has transferred to the user the right to execute on the condition that a certain terminal date had not passed, (i.e. the user has the right to execute the protected application up to, but not after March 1, 1987). The coprocessor's operating instructions necessarily, therefore, provide for storage of a last allowed use (terminal) date along with the software decryption key. Since the coprocessor maintains a real time clock, whenever the decryption key is accessed or at intervals during application execution, the terminal date and the current date are available. The terminal date provision is protected against unauthorized alteration by the security of the coprocessor as is the real time clock setting. The encrypted portion of the software (the protected portion) describes the criterium that execution is not available beyond the terminal date. Whenever the protected software is run, the decryption key and the terminal date are accessed from the coprocessor's non-volatile memory. The criterion tested in the protected software requires that the terminal date be compared to the current date; if the current date is beyond the terminal date, then execution of the protected software does not proceed. The protected software can also be arranged to provide for deleting the particular soft-

ware decryption key in the event that the current date is beyond the terminal date. It should be apparent to those skilled in the art that another condition which can be substituted for the terminal date condition is the number of times the software is executed. For this case, the protected software describes the number of executions which have been authorized, and in lieu of storing the current date along with the software decryption key, a count of allowed uses is stored which is decremented each time the software is executed. The protected portion then tests the allowed number of executions against the criterion that the number is greater than zero. It then either decrements the number or, if the number of authorized executions is zero, denies the user's request to execute the software (and perhaps the software decryption key is also deleted). It should be apparent that there are many variations to these specific implementations, including elapsed time, passwords, and combinations of these and other measurables, all of which are within the scope of the invention.

Transfer of Right-to-Execute

Transferring the right to execute from one user to another (or more particularly, from a source coprocessor to a sink coprocessor) can be accomplished by reconstructing a distribution set. This procedure returns the right to execute to a portable form which is substantially identical to that from which it was acquired in the first place, see copending application [YO985-091]. This procedure, necessarily, removes the right to execute from the source coprocessor.

This transaction requires that the user obtain either a token or a disk and a token pair (also referred to as a Transfer Set), depending on the structure of the token. These sets can be provided by the hardware vendor. The token (or cartridge) in the set is loaded by the coprocessor hardware manufacturer. The Transfer Set, prior to manipulation by the user has a single piece of information, token data, stored in two forms. The token is loaded, by the hardware vendor with clear text token data; the physical characteristics of the token protect this sensitive information from unauthorized persons. The same data is encrypted under a hardware manufacturer secret key called a Common Supervisor Key (CSK) to generate $E_{CSK}(\text{token data})$. It is stored either on the disk of the Transfer Set, or in the token if it is so structured as to allow it. Because $E_{CSK}(\text{token data})$ is encrypted, it may be stored on the disk even though in that form it can be read and even copied by anyone. It is necessary that the transfer set be prepared by a trusted source, such as a hardware vendor, be-

cause if the token contents are known, other tokens could be loaded with known contents and the transferred right to execute replicated. Assuming that the user has acquired a suitable transfer set, the distribution set is prepared using a Reconstruct Distribution Set (RDS) process, by the user and his composite computing system, for example, as follows.

A utility program, running on the host computer, signals the (source) coprocessor that an RDS sequence is about to begin. The utility program identifies to the coprocessor the location of the key to be transferred. The coprocessor executes a CBS (Create Backup Set) procedure on all allowed keys except the indexed key. The CBS procedure is described below. At this point it is sufficient to note that the CBS procedure invalidates any existing hardware backup mechanism. The coprocessor requests and receives a copy of the encrypted token descriptor $E_{CSK}(\text{token data})$ from the transfer set. The coprocessor decrypts the token descriptor to provide clear text token data. This clear text token data is then encrypted using the software decryption key identified by the index to produce $E_{AK}(\text{token data})$. The coprocessor then stores this encrypted token descriptor $E_{AK}(\text{token data})$ in a reserved non-volatile storage area of the token or on the disk and either erases or otherwise de-activates the software decryption key AK at the given storage location. The coprocessor then passes the encrypted token descriptor to the host for storage on the transfer set disk. As will be described later, the key (AK) to be transferred may be associated with conditions of execution. If these conditions of execution are unchanging (such as terminal date) then the encrypted application key may be copied to the transfer set disk. If the conditions of execution are changing (such as remaining hours of use or remaining number of uses), then the encrypted file containing the application key and the conditions of execution cannot be copied from the distribution disk without resetting the conditions. This synchronization of a token descriptor file and an application key file can be achieved by including a correspondence test number in each file. The next step in transfer is thus the preparation of an encrypted application key file for storage on the transfer disk. This preparation is identical to the encrypt vendor key (EVK) transaction described below save that the correspondence test number is substituted for the random number. This correspondence number could be a fraction of the token data. After this preparation and transfer, the utility program, running in the host, then transfers to the transfer set disk the two files containing the plain text and cipher text parts of the protected program. The reader can now verify that the distribution set is

identical to the distribution set described in EP-A-..... [YO985-091] in that it includes the encrypted token data, encrypted with the software decryption key AK, the plain text file and the protected or encrypted software file, also encrypted under the software decryption key AK, as well as the software decryption key AK encrypted by the hardware vendor's key CSK. The latter three elements may be copied from the original distribution disk or any backup copy of those files if permitted by execution conditions. It should be self-evident that since the distribution set is now identical in all but one respect, it is usable with any coprocessor to transfer the right to execute the particular encrypted software file. The only difference between the distribution set and the original set from which the right to execute was acquired, is that the token data is very likely to be different; this is immaterial as long as both portions of the set (the token cartridge and the diskette) have been derived from identical token data. The (source) coprocessor now deletes the decryption key AK from its temporary memory. At this point, the right to execute has been deleted from the source coprocessor and exists solely in the Transfer Set.

Transfer of the right to execute, however, need not be indirect, e.g. through the transfer set already referred to. Transfer of the right to execute can be direct, e.g. using a coprocessor to coprocessor communication link. Furthermore, the coprocessor to coprocessor communication link need not be secure in order to maintain the safety of the right to execute being transferred; rather the safety is cryptographically secured as will now be described. In the following discussion we will refer to a transfer from coprocessor to coprocessor, however, the reader should understand that the communication link between coprocessors can either be through direct connection, or can be through any bidirectional data communication system. A transfer of a right to execute from one coprocessor to another is considered safe when the two coprocessors involved are able to identify one another as "members of the family" and generate a one time only Session Key for their use in that transaction. The identification as members of the family is needed for assurance that the procedures used by each will mesh correctly, so that proliferation of rights to execute will not occur, and so that other protected information will not be revealed.

The transaction in which the Session Key is generated relies on the presence of information in high privilege memory which is common to the two coprocessor systems participating in the transaction and on the ability of coprocessors to generate good random numbers. The process which generates a Session Key will result in both coprocessors involved in the transaction possessing the

same key only if both coprocessors have the necessary antecedent information in common.

The transaction for mutual identification and generation of a Session Key is as follows. For purposes of this description we will refer to the user or the user's composite computing system or the user's coprocessor as the source user, source composite computing system or source coprocessor if the right to execute is being transferred from that user, composite computing system or coprocessor. We will refer to the user, composite computing system or coprocessor as the sink user, sink composite computing system or sink coprocessor if the right to execute is being transferred thereto. The source user signals the source coprocessor that a Session Key is needed. The source coprocessor generates a random number which will be used in generating the session key, pads it with another random string of bits, and appends a Message Authentication Code (MAC). The MAC can be used to ensure that the plain text message which is recovered on decryption is identical to the one transmitted. The source coprocessor then encrypts the number with a key CSK and sends the encrypted number to the sink coprocessor. The sink coprocessor has performed the same function and has sent its random encrypted number to the source coprocessor. The source coprocessor decrypts the number received under the encryption key (CSK). In the event that each coprocessor stores multiple CSKs, then each coprocessor decrypts the received number under each CSK in succession until either a valid MAC is obtained, or the collection of supervisor keys (CSK) is exhausted. If a valid MAC is not found, then an error message is returned. This will be the typical outcome if a processor which is not a "member of the family" tries to pass itself off as one. If a valid MAC is obtained, then the random numbers generated in the two coprocessors are combined in both coprocessors and are used as the Session Key. Of course, part of the operating instructions for the coprocessors will define, a priori, the particular manner in which the random numbers are to be combined in order to generate the Session Key; one number could be concatenated with another; the numbers could be EXCLUSIVE-OR'ed, etc.

In order to avoid the procedure which may require successive decryptions in a search for the "correct" supervisor key, location information such as an index for the supervisor key which had been used could be sent along with the encrypted number. There is an advantage, however, to the technique which requires coprocessors to "search" for the correct supervisor key. A procedure which transmits an index number along with the encrypted number provides a growing collection of in-

formation about the supervisor keys to any observer.

Once the Session Key has been generated, it is possible for the coprocessors to transfer rights to execute by encrypting them under the Session Key. The coprocessors' firmware, controlling the procedure, ensures that the rights are erased from the source processor. The right to execute could be erased when transmitted by the source processor, although a preferable technique is to erase the right to execute (the software key) only when the sink coprocessor indicates that the right to execute has been safely received and to activate the right to execute only when the source coprocessor indicates the right to execute has been deactivated. The right to execute, which is transferred in encrypted form, is secured against an observer by its encryption and there is no need to employ a secure communication link or channel.

Direct or inter-coprocessor communication is the method of choice for movement of rights to execute in a network or a mainframe link environment. In these cases or others involving placing more than one right to a particular application in a particular coprocessor, a count of the rights for a given package is maintained in the key storage area of the source coprocessor so that the number of rights which have been received limits the number which are distributed.

It should be clear from the above descriptions that it is within the realm of this mechanism to associate with an AK a description of the life span of an AK in several dimensions (time, numbers of use, etc.). It should also be clear that it is within the capacity of this mechanism to divide or parcel out this span under control of software provided by the software vendor and executed by a coprocessor. Libraries of software could be maintained in distributed computing systems by these means without violating the conservation of rights to execute while providing benefit to the distributed computing system's user.

In the event that a transfer of multiple rights to execute is required, the coprocessor to coprocessor transfer proceeds as follows once a Session Key has been created. The source user identifies to the source coprocessor those rights to execute (AKs) to be transferred. The source coprocessor executes a CBS procedure (defined hereinafter) in order to update any backup set of rights to execute. The source coprocessor then encrypts the software keys under the Session Key and stores them with the Session Key in a reserved location of temporary memory. The source coprocessor marks each software key from the key store (permanent memory) as inactive and sends the encrypted information to the sink coprocessor. The sink coprocessor receives the collection of encrypted

keys from the source coprocessor, and decrypts them under the Session Key. The sink coprocessor then stores the decrypted keys in its key store (permanent memory) marking them inactive and sends its host computer location information by which the applications can access the keys in the load decrypt run procedure. The files actually comprising the protected software can be sent by any conventional (unprotected) technique or apparatus. The sink coprocessor can return a message to the source coprocessor indicating receipt of the particular software key or keys to induce the source coprocessor to eliminate those software keys from its temporary memory. When the source coprocessor confirms the removal, the keys are then activated by the sink coprocessor.

It should be noted that a software vendor may not wish to allow transfer of a right to execute and that this constitutes a term or condition of sale. Conditions which control the allowed movement of rights to execute can be stored in association with an AK as part of the procedure in which it is acquired. If a manipulation of an AK is requested by a user, then these conditions (flags) are tested against go/no-go criteria stored in the coprocessor firmware which implements the requested manipulation.

Backup of Right-to-Execute

The backup procedure to be described is one which is intended to insure that the collection of rights to execute stored in a user's coprocessor are not lost due to an unforeseen failure of, for example, the supply of power to the coprocessor's non-volatile memory. This is to be distinguished from backup procedures which are applied to files of data and software. The latter procedures are entirely conventional, well understood, and are applicable to those kinds of objects, where they exist, in this system (plain text and encrypted software and encrypted application key). Many functional copies of such objects may be kept for use by any authorized system, thus ensuring against their loss. It is, rather, the objective of the backup procedure described below to back up rights to execute so that they are not lost but so that many functional copies of that kind of object cannot be made.

Because the backup procedure is designed to circumvent the results of an unforeseen failure in the coprocessor, the backup procedure must create, external to the coprocessor, sufficient information so that the right to execute can be installed entirely independently of the (source) processor which stores an entirely valid right to execute. Because of this necessary independence, the backup procedure itself is a potential source of a

(duplicate or spurious) right to execute. Allowing the creation of backup rights is a policy decision for the software vendor. It is a potential detriment to his security and would be provided for his customers' convenience. As noted earlier with respect to transfers of rights, a provider of software may not wish to allow backup. This condition of sale is enforceable by the same mechanism as described for control of transfer given the existence of a no-backup flag associated with an AK. This option is desirable in the case that the conditions of execution may change. To minimize the impact of backup rights, they are, in this system, made conditional in that they expire after a conveniently short interval which is long enough for the user who has actually had a failure in his coprocessor to have that failure verified, for example by the hardware manufacturer.

Assuming the hardware manufacturer verifies the failure of the user's coprocessor, the means are provided to the user to carry out an additional procedure to remove the condition on the backup rights. In order to safely integrate the creation of backup rights with the other capabilities described herein, the creation of backup rights should be thought of as beginning a transfer of all allowed rights which is then left pending completion. Transfer procedures are necessarily interrelated with the backup procedures so that any user backup set (which carries a potential right to execute) is invalidated at the time any complete transfer is effected. This prevents the transferred rights from also being present in a valid backup. Accordingly, the user has the following options in connection with the procedures described herein:

1. With his right to execute installed on a coprocessor, the user can have a backup set (representing a collection of potential rights to execute) which can be converted into an actual, but conditioned, right to execute, or

2. The user can remove one or more rights to execute from his coprocessor and install them in a transfer set or directly transfer them to another coprocessor, but that procedure requires invalidation of the existing backup set. This requirement is entirely consistent with the user's rights since when rights to execute are removed from a coprocessor, there is no need for the rights to be represented in the backup set. Obviously, a new backup set which correctly reflects the diminished set of installed rights to execute may be prepared immediately after a transfer.

The procedures arranged for creating backup rights are comprehensive in that a single backup set can retain potential rights to execute for multiple applications. The procedures contemplate that the user's collection of rights on execute may be dynamic, e.g. his collection of rights on one day

may be greater or less than his collection of rights on another day. This necessarily requires that the backup rights be dynamic too and track changes in the user's collection of rights to execute.

Basically, the backup procedure is a two-step process, in a first step a Backup Set is created (Create Backup Set, or CBS); the Backup Set includes a disk on which an encrypted file of rights to execute (for a group of applications) is stored. A supervision key which is unique to this (source) processor (USK) is also included in this file. This information will allow the hardware manufacturer to verify that the failed processor which they receive as evidence of the failure is the processor claimed to have contained these rights. A token which can validate this collection to a coprocessor is also part of the set. The key used to encrypt this file is a random number generated by the coprocessor, possibly by encrypting the date and time with a unique supervisor key (USK). It is the authorization to use this random number (RK) key which is validated by the backup set token. As noted above, the Backup Set is considered a pending transfer.

The second step in the backup process is Install Backup Set (IBS); in this step the potential right(s) to execute represented by the backup set, consisting of the token and disk, is installed on a coprocessor. Because it is contemplated that the user is likely to execute the CBS step of the backup procedure on plural occasions before ever executing the IBS step, the token which is employed in the Backup Set must be more capable than the token used in the Distribution Set; this capability is required because of the fact that the user may execute the CBS step each time a new application is acquired. The user's existing backup must be invalidated at that time to prevent the creation of additional rights to execute. Accordingly, the token data will typically be much longer than the token data used in a Distribution Set so that a portion of that token can be read as part of each CBS transaction, changing the token content as a consequence, and invalidating previous backup disk files, without in the process completely discharging the token. The same token may then be used for the IBS transaction if or when it is needed. It is presently contemplated that rather than employing shift register storage on such a Backup Set token, storage will be designed around random access memory. The description which follows however will for simplicity assume that the backup token is based on shift registers as in copending application [YO986-010], but containing extra length shift registers.

Prior to initiating a CBS step, the user has acquired a Backup Set consisting of a token and a disk. The disk, as acquired by the user, stores encrypted token data, $E_{CSK}(\text{token data})$. The token,

as acquired, stores clear text token data.

The CBS step proceeds as follows:

A utility program signals the coprocessor that a CBS sequence is about to begin.

The coprocessor requests and is given the encrypted token data corresponding to the token portion of the Backup Set.

The coprocessor decrypts the token data and selects the amount of the token data that will be used. "Use" of a portion of the token data implies that this portion of the token data will be destroyed; the remaining portion of the token data is available for subsequent executions of the CBS procedure, for example when the user obtains a subsequent application, the rights to which he desires to backup.

The coprocessor generates a random number of length equal to the amount of the token data to be used and employing the random number "reads" or challenges the token and obtains the token response. Since the coprocessor already has available to it the clear text token data and the random number it has generated, it can predict or compute the correct response. The computed response and the actual response of the token are compared. If the comparison indicates that the token response and the computed response do not correspond, then an invalid token has been presented, an error message is returned, and the sequence terminates. Assuming, however, that the computed and actual responses correspond, then the transaction continues. By reading or challenging the backup token, the token data contained therein is changed (as well as verified). Changing the token data invalidates all copies of any previous backup. Thus the necessity for the length of the token; it can only be used a number of times given by the ratio of the bit length of the token portion to the portion used each time the CBS step is executed. When the token contains only enough data for one more transaction, it may be read to be destroyed and a new backup token may be started.

For the remainder of this transaction, it is assumed that the cryptographic system employed in the coprocessor allows any number to be a valid key. Random numbers are thus valid keys. This property is a characteristic of the DES system.

Having verified the authenticity of the token, the coprocessor now encrypts, under a second random number, the remaining, unused portion of the token data, the allowed portion of its key store and the unique supervisor (USK) key which identifies that source processor. The encrypted block, as described, can then be stored on a disk. This file will be used for the Install Backup Set procedure.

A copy of the random number used as an encryption key above is now encrypted under a

supervisor key using the encrypt vendor key procedure. This datum is now stored on the backup disk.

These files can be copied in the same way the protected software can be copied, i.e. an unlimited number of times. However, the file is usable only with the token and then only in the event the token has not been read in the interim. As already described, any subsequent transfer operations require invalidating the token. The Install Backup Set step is now described, assuming that the user has access to both the file that was created during the last execution of the CBS step, as well as the token, which has not been read in the interim.

We also assume that in the interim the user's coprocessor, the source coprocessor, has failed, but the user has available another (sink) coprocessor. The Install Backup Set procedure will install, on the sink coprocessor all the rights to execute that had existed on the user's source coprocessor (to the extent backup was allowed). However, in order to protect the software vendors, the entire collection of rights to execute will be conditioned by a grace period. During the grace period, each of the rights to execute will be operative and the user can employ them as he would have in his (source) coprocessor. During the grace period, the user can return his failed (source) coprocessor to the hardware vendor. The hardware vendor, after verifying that the coprocessor has indeed failed, will provide to the user a disk having an encrypted message verifying, to the (sink) coprocessor that the (source) coprocessor has failed so that the grace period condition on the rights to execute can be lifted. Accordingly, the IBS step includes two sub-steps; a first sub-step installs the rights to execute in the (sink) coprocessor. At the time these rights to execute are installed, they are conditioned so they become ineffective at the expiration of a grace period. The second sub-step in the IBS step is removal of the condition on the rights to execute by employing a disk acquired from the hardware vendor. The IBS step then proceeds as follows.

A utility program signals the sink coprocessor that an IBS sequence is about to begin. The coprocessor first requests, and is sent, the encrypted random number key which has been used to encrypt the backup file. This is decrypted under the appropriate CSK. The coprocessor then requests and is given the encrypted backup file. The encrypted backup file includes the encrypted token data, the contents of the key store from the (source) coprocessor and the unique supervisor key of the source processor.

The (sink) coprocessor decrypts the backup file using the random number key found in the previous step, removes the token data and verifies the token. Token verification proceeds as in verification of the Distribution Set, i.e. the verification

changes the token contents. As a result, the token can be used to perform an IBS procedure only once. Assuming the token is valid, the set of backup rights to execute is installed in the permanent memory of the (sink) coprocessor, along with an expiration date, thus determining the extent of the grace period.

A message is now prepared by the (sink) coprocessor containing a copy of both coprocessors' unique keys. This message is returned with the failed source coprocessor so that the condition-lifting message from the hardware vendor can be identified by the sink coprocessor as intended for it, and as intended for the set of rights to execute of the particular source coprocessor.

At this point, the (sink) coprocessor is in the same condition that the (source) coprocessor was at the time it was last backed up, except that all the rights to execute are conditioned on the expiration date. Assuming that the user obtains, from the hardware vendor within the grace period, the verification disk, the second sub-step of the IBS step proceeds as follows.

A utility program signals the (sink) coprocessor that an IBS sequence is about to be completed. The (sink) coprocessor requests and receives the validation file and decrypts it under its supervisor key (the USK of the sink). If the file contains the unique key which identifies the (source) coprocessor, then the condition is lifted. If the file does not contain the unique key of the (source) coprocessor, then an error message is returned and the sub-step is not completed.

Backup Through Inter-Processor Communication

In the preceding, the "hardware" backup has been described as comprising the CBS and IBS procedures, both of which rely on an extended token. Use of a token or extended token however, is not essential to "hardware" backup, and an intermediate coprocessor can be employed in lieu of the token or extended token for "hardware" backup purposes so long as the intermediate coprocessor can be arranged to firstly communicate with the source coprocessor (for the CBS procedure) and then communicate with a sink coprocessor (for the IBS procedure).

The inter-processor variant of the "hardware" backup procedure is now described.

For this description, we assume that the source coprocessor is in communication with the "intermediate" coprocessor. The coprocessors initially exchange encrypted random numbers, each encrypted under a supervisor key selected by the transmitting coprocessor. As already described, each of the coprocessors can decrypt and recog-

nize that it has decrypted the encrypted random number transmitted by the other coprocessor even though it is not initially aware of the specific supervisor key employed. Assuming that each of the receiving coprocessors successfully decrypts the encrypted random number, they both combine those clear text random numbers to generate the Session Key which will be used for subsequent communications.

The source coprocessor then extracts the application key (AK) or keys sought to be backed up from its permanent memory and encrypts that key information and its USK under the Session Key to generate an encrypted key block. This is stored on a backup disk. The Session Key is stored by the intermediate coprocessor in its secure memory along with a descriptor indicating that the key corresponds to a backup set. At this point the intermediate coprocessor has possession of the key needed to access the AK or AKs which are being backed up and were it not a trusted recipient, it could generate spurious rights to execute. However, the identification procedure referred to above has identified, to the source coprocessor that the intermediate coprocessor is a "member of the family". As such a member of the family, the logical and physical security of the intermediate coprocessor protects the right(s) to execute which have been transferred from spurious duplication or use. The actual encrypted application(s) can be transmitted to the intermediate coprocessor for the IBS procedure, by any conventional means.

If at a subsequent time the source coprocessor is requested to transfer right(s) to execute which have been backed up via an "intermediate" coprocessor, as already described that transaction cannot take place until the source coprocessor communicates with the "intermediate" coprocessor to invalidate the backup rights. Such communication has only three essential components. The first component is the identifier sequence as already described. This satisfies the source and intermediate coprocessors that the communicating parties are indeed "members of the family". The second component is the transmission from the source coprocessor to the intermediate coprocessor of a message requesting invalidation of the backup rights key. The third component is the reply from the intermediate coprocessor that it is indeed the intermediate coprocessor which stored the backup rights and that the rights have been invalidated.

The backup rights stored in a "intermediate" coprocessor can either be installed, using an IBS procedure, in the intermediate coprocessor, or can be installed in a different (sink) coprocessor. If the backup rights are to be installed in the intermediate coprocessor, that action is readily effected by a user request through the host associated with the

intermediate coprocessor; the rights are installed without requiring a token but, as already described, those rights are conditioned on the grace period.

In the event that an IBS procedure using an intermediate processor is performed, the processors first establish their mutual identities as "members of the family" by establishing a session key. The random key may then be encrypted under the session key and transferred to the sink coprocessor. The sink coprocessor is thus authorized to install the set of backup rights to execute with the grace period and prepares a message for the hardware manufacturer as previously described.

Encrypt Vendor Key

As described both in this application as well as in copending EP-A-..... [YO985-091], the coprocessor is also used to provide a service to a software vendor of encrypting the software decryption keys (AK). It is essential to the protection provided by the entire software copy protection system that the supervisor keys (CSK) which are used to encrypt the software vendor's decryption key be maintained secret. By allowing the software vendor the use of a coprocessor and the ability to encrypt an unlimited number of keys, the software vendor is in a position to mount a conventional "chosen plain text" attack on the hardware vendor's encryption keys (CSK). In the event that a software vendor were able to learn the hardware vendor's keys (CSK), that software vendor could use those keys in an attack on encrypted software of other software vendors. The "chosen plain text" attack requires that the attacker have access to sets of corresponding plain text and cipher text. Using these sets the attacker may attempt to identify the key which will produce the cipher text from the plain text or visa versa. The difficulty of doing this is, of course, dependent on the cryptographic system chosen and the computing power available to the backtracking task. Some cryptographic systems (such as DES) are extremely resistant to unlimited plain text attacks.

In a first limitation on use of the coprocessor in a plain text attack, the coprocessor is arranged so that the software vendor requires authorization from the hardware manufacturer in order to create rights to execute. This authorization is sold, by the hardware vendor to the software vendor. Accordingly, one limitation on the software vendor's use of the coprocessor in a plain text attack is the economic cost expended in generating sets of plain text and corresponding encrypted text. Another technique is the use of the following Encrypt Vendor Key (EVK) procedure.

A utility program signals the coprocessor that an EVK sequence is about to begin. The coprocessor requests and is given the key (AK) to be encrypted, typically a software vendor's key. The key is supplied by the software vendor along with desired settings of supervisor flags. These flags control whether or not the supervisor will allow (for example) backup or transfer of the associated key.

The conditions of the execution which will be examined and/or changed by the application key are also supplied. It should be understood that in the following discussion AK refers to the entire datum (flags, key and conditions) to be prepared for transfer by this process.

The coprocessor generates a random number (RN) and uses it to pad the front end of the key AK. The coprocessor pads the back end of the key with a recognition flag (RF). As previously described, the RF may be a MAC of any kind which is appropriate both to verifying that the correct CSK has been used (during decryption) and to the cryptographic system employed by the coprocessor. Both the random number and the recognition flag are unknown to the user, e.g. the software vendor. The coprocessor encrypts the resulting block under a supervisor key (CSK) and passes the result back to the utility program. The result, $E_{CSK}(RN.AK.RF)$, where "." represents string concatenation, i.e., 01.111 produces the string 01111, can be decrypted by any coprocessor that is aware of CSK. The result of such a decryption $RN.AK.RF$ includes the three components, i.e., a random number (RN), the decryption key (AK), and a recognition flag (RF). The decrypting coprocessor can always identify AK so long it has a priori access to the length of the suffix recognition flag. The random number padding assures that even if the same key (AK) is submitted many times, the resulting blocks and the encrypted results will be different thus foiling the plain text attack. The EVK procedure has another advantage in that so long as the decrypting coprocessor has a priori knowledge of the recognition flag (RF) it can decrypt the encrypted block without specific a priori knowledge of CSK so long as it has a priori knowledge of all possible CSKs. More particularly, assume that each coprocessor is provided by the hardware vendor with CSK1-CSK5. If appropriate measures are taken to avoid cryptanalytic attack one can further assume that the recognition flag (RF) which is used is always the encryption key itself. These measures must in the case of block ciphers include that the RN is not an integral number of blocks in length. Further assume that the encrypting coprocessor randomly selects CSK3 with which to encrypt a particular software key AK. Thus the encrypted block is $E_{CSK3}(RN.AK.CSK3)$. Any other coprocessor having access to CSK1-5 can correctly decrypt this block

even though it is not aware which of the keys CSK1-5 have been used. It is only necessary for the coprocessor to decrypt the encrypted block with each of the keys CSK1-5. In only one instance will the plain text version include, as a suffix, the decryption key actually used.

Virtual Key Storage

In any practical implementation of the software protection mechanism described herein and described in [YO985-091], there must be some limit to the ability of the coprocessor to store rights to execute. If a user obtains such a number of rights to execute greater than can be stored in the coprocessor, the user could convert seldom used rights to execute back to transportable form through the transfer transaction. The act of swapping AKs into and out of the coprocessor by these methods could easily prove burdensome to users and would be contrary to the spirit of this mechanism. It is easy, however, given the resources of the coprocessor, to overcome this problem.

In the simplest case, the AK represents the right to access the services of a piece of software. Extending this concept slightly, a Meta-AK (MAK) may be thought of as representing the right to access a collection of rights to execute. This sort of Key has already been seen in a limited form in the RK or random key used in the backup transaction.

Assuming a user has filled all the key positions in his processor and wishes to install yet one more, the coprocessor can give the user the option of starting a file of keys on a system disk (hard or floppy). This collection of virtualized keys is stored in an encrypted form under a MAK. Each time the collection is accessed to move or add an AK, the collection is re-encrypted under a new random MAK. The MAK is stored in the key store and is marked as a MAK in the flags which control backup and transfer to facilitate its correct handling by the processor. The change of MAK on each access is needed to keep the virtualized key store which is used by the processor synchronized with the actual collection of rights to execute possessed by the user. Copies of old virtualized key stores which contain transferred virtualized rights to execute cannot be foisted on the coprocessor because they will not decrypt correctly on loading.

A specific procedure for creating virtualized keys (for the purpose of freeing up key storage) proceeds as follows. A utility program running on the host signals the coprocessor that the user has requested creation of a virtualized key. The coprocessor requests the user, via the host, to identify by location information, the AKs which should be included within the virtualized store.

Based on the user identification, the AKs identified are extracted from the key store along with their flags (identifying authorization for transfer, backup, etc.), conditions of execution and location information. The coprocessor generates a random number and encrypts the block consisting of that data. The resulting encrypted block can now be written to disk (hard or floppy). The random number (the key to the virtualized store) is then written in the permanent memory in place of one of the AKs which has been virtualized. A key reference path file which maps the virtualized keys to the random number MAK index can be provided in plain text to an access utility on the host to allow reference ambiguity to be resolved. This file associates the random number key with the location information identifying the AKs which have been virtualized. If the user, at any later time, requires execution of software protected by one of the virtualized keys, the coprocessor first attempts to use the key at the referenced location. The correctness of the key found in that location can be tested by conventional message authentication techniques. This key verification can be performed by loading and decrypting a short message file with an authentication section (provided as part of the protected program). If on decryption the authentication is valid, the correct key has been found. If the authentication is invalid then the access utility can provide a list of virtualized key access paths which will contain the key if the user indeed possesses that key. These keys are obtained by decrypting the virtualized block and extracting the appropriate AK. These keys may then be tested for validity by repeating the authentication procedure described above. At this point the coprocessor has access to the selected, previously virtualized AK.

Clearly a virtualized key store could itself contain MAKs so that the size of the key store can be extended indefinitely.

Demonstration Software

The virtualized storage technique also provides for supporting demonstration software without the need for any validating mechanism such as a token source or cartridge. The transaction proceeds as described below. The set of flags which allow or disallow transfer and backup of keys includes a further flag which allows or disallows erasure of keys. If an AK is to be accepted in the absence of a token, then the data files for loading that AK include a null token descriptor so that the empty token connector will respond correctly to the token query. The flag settings for this particular AK include settings that allow it to be backed up and do not allow it to be moved or erased. Installation of

such an AK also requires a search of both installed and virtual key stores to see if this key had been installed before.

Conditions for executing demonstration software (preferably) include elapsed time or number of uses. An AK installation which proceeded under conditions as described above would allow a person to acquire the right to execute a piece of software for demonstration purposes, typically a one time use. A second attempt to install the identical AK would detect the prior acquisition, since the key store is searched and the key cannot be moved or erased. The user is protected from filling his key store with useless demonstration keys by having them virtualized. The software vendor is protected from having his code reinstalled repeatedly, using demonstration software, without control.

Brief Description of the Drawings

The present invention will now be described in such detail as to enable those skilled in the art to practice the same in the following portions of the specification when taken in conjunction with the attached in which like reference characters identify identical apparatus and in which:

Fig. 1 schematically identifies the important components of the software asset protection mechanism and how they interact;

Figs. 2-4 are similar to Fig. 1 but are useful in explaining the use and application of conditioned rights-to-execute;

Figs. 5-7 are similar to Fig. 1 and are useful in explaining transfer of a right to execute;

Figs. 8-16 are similar to Fig. 1 and adapted to illustrate the two steps of the backup procedure, particularly Create Backup Set (CBS) and Install Backup Set (IBS);

Fig. 17 shows a typical time sequence in employing the CBS and IBS procedures;

Fig. 18 is useful in explaining the Encrypt Vendor Key (EVK) procedure;

Fig. 19 is useful in explaining the appearance of a key store illustrating several features of the flags and conditions accompanying keys; and

Figs. 20 and 21 are useful in explaining a direct transfer of a right-to-execute.

Detailed Description of Preferred Embodiments

Reference has already been made to copending application [YO985-091], the disclosure of which is incorporated by this reference along with YO986-010 (disclosing an example of a token). Application [YO985-091] discloses the basic soft-

ware asset protection mechanism. That mechanism will be briefly reviewed in connection with Fig. 1. The software asset protection mechanism requires that the user employ a composite computing system including a host 10 and a coprocessor 20, connected via some communication link or path 14. As described in [YO985-091], the path 14 may be an internal bus, e.g. enclosed within the covers which encompass both the host 10 and the coprocessor 20, or the path 14 can comprise a link between an I/O device included within the coprocessor 20 and an I/O device associated with the host 10. Regardless of the specific nature of the link 14, the coprocessor 20 is provided with physical security which is effective to prevent mechanical tampering or access to the interior of the coprocessor 20 by a user or a pirate. That physical security is represented in Fig. 1 by the interior dashed line boundary. Two important features of the coprocessor 20 are its permanent, non-volatile memory 25 and a temporary memory 26; the latter akin to the working memory (RAM) of a conventional computer. The coprocessor 20 is provided to the user in a form in which it has at least one decryption key CSK stored in the permanent memory 25; the decryption key CSK is provided and stored by the vendor of the coprocessor 20. In order for the user to execute a protected application, he must install a right to execute the application in the permanent memory 25; this right to execute is represented by a software decryption key AK. As described in the application [YO985-091] the user, in order to install the right-to-execute, receives from the software vendor a distribution set which includes a hardware cartridge 30 and a distribution disk 16. As shown in Fig. 1, the distribution disk 16 typically stores three files; of these files, one is the protected application. Typically the protected application will appear as two parts in two sub-files, a plain text application file A and an encrypted or protected portion application file B. As Fig. 1 shows the application file B is encrypted under the software decryption key AK. A second file on the distribution disk 16 is the software decryption key, encrypted under the key CSK. Finally, the last file on the distribution disk is token data, T₁, encrypted under the software decryption key AK. As is also explained in [YO985-091], it is not essential that the third file be incorporated in the distribution disk 16 and alternatively it may be incorporated in the hardware cartridge 30.

The hardware cartridge stores the token data, T₁, in plain text form. Like the coprocessor 20, the hardware cartridge 30 is provided with physical security. To install the right-to-execute, the hardware cartridge 30 is coupled to or linked to the combined computing system; Fig. 1 represents this

coupling via a connecting cable 18. The coprocessor decrypts the software decryption key AK in temporary memory. Before accepting the software decryption key AK into permanent memory, the coprocessor 20 verifies that the hardware cartridge 30 is authentic in a forgery-resistant query/response transaction (since its contents, T_1 , correspond to the encrypted file $E_{AK}(T_1)$). The hardware cartridge 30, because of its destructive read property, will only contain the token data, T_1 , if it has not been used. After verifying that the hardware cartridge 30 is both authentic and unused (and destroying the utility of the hardware cartridge in this process) the coprocessor will accept the right to execute, and store in its permanent memory 25 the software decryption key AK. With access to the software decryption key AK, the protected application file B can be decrypted and stored in the temporary memory 26 of the coprocessor 20 so that it may be executed by the coprocessor 20. Because of its physical and logical security, the plain text form, in which application file B is stored in temporary memory 26 during the course of execution and is not available to the user or a pirate.

Conditioning Rights to Execute

The software asset protection mechanism, as briefly described above, installs an unconditioned right to execute in the coprocessor 20. However, it is one of the features of the invention that the right to execute can be conditioned, and examples of conditions are terminal dates and times, or numbers of executions. Fig. 2 is similar to Fig. 1 except that in the case of Fig. 2 the protected portion of the application file includes a criterion for execution, e.g., if the terminal date and/or time is later than the present date then execution is allowed. On presentation of a distribution set as shown in Fig. 2 to the combined processing system of the host 10 and the coprocessor 20, the installation of the right to execute proceeds exactly as was described in connection with Fig. 1. The coprocessor 20, via the agency of the host 10, verifies (and destroys) the token 30 by comparing its plain text contents (T_1) with a decrypted version of the file $E_{AK}(T_1)$ read from the disk 16. On verifying the authenticity and the previously unused nature of the token 30, the coprocessor 20 stores the software decryption key AK in the permanent memory 25. The conditions of execution can be stored in the same file as the AK and can be installed at the same time as AK. In the case shown in Fig. 2, the coprocessor 20 stores the datum which can be interpreted as a terminal date and/or time. This interpretation will be performed by the protected part of the application on

any occasion of its use. The terminal date storage is associated with the software decryption key AK, as shown in Fig. 3. More particularly, Fig. 3 is entirely identical to Fig. 2 except that it shows the software decryption key AK, and the terminal date and/or time, stored in the coprocessor 20's permanent memory as well as indicating that the token 30 has been depleted. Thereafter, each time the protected application is run on the coprocessor 20, prior to authorizing execution, the application uses the criterion stated in the encrypted application file that the current date and/or time not be later than the terminal date and/or time and only authorizes execution in the event the criterion is met. The current date and/or time is supplied on demand by the coprocessor 20 to the executing application.

Fig. 4 is similar to Fig. 3 except that the conditions stated in the encrypted application key file gives the remaining number of authorized executions. On installation of the right to execute, the software decryption key AK is associated with a count C; each time execution of the application is requested, the contents of the count C is tested against the criterion that the number C of authorized executions remaining is greater than zero. The count C is then decremented. Only so long as C is greater than zero will execution be authorized.

It may be advisable, regardless of whether or not the condition is a terminal date and/or time, or a number of executions, to provide the coprocessor 20 with instructions to delete the associated software decryption key AK, once the initial conditions are no longer met. Thus, the software decryption key AK is automatically removed from the permanent memory and thus the right to execute is deleted.

Figs. 5-7 are useful in illustrating transfer of the right to execute. As shown in Fig. 5, the coprocessor 20 has installed the right to execute a particular protected application in the form of the software key AK in its permanent memory 25. The user, in order to effect the transfer of the right to execute, obtains a transfer set. The transfer set includes a token 40 and an accompanying disk 46. The token 40 had been loaded via a trusted source such as the coprocessor hardware manufacturer with token data T_2 , and the disk is written with the token data encrypted under the hardware vendor's key so the disk stores the file $E_{CSK}(T_2)$. The user also has available his original source disk 16 which includes the files enumerated in Fig. 5.

Fig. 6 shows the condition of these components after the first step in the transfer sequence has been completed. More particularly, the disk 46 of the transfer set is read, and its contents are decrypted so that the coprocessor 20 can store, in its temporary memory 26 the token data T_2 . The software decryption key AK to be transferred, is

moved from the permanent memory 25 to the temporary memory 26.

The next step in the transfer sequence is to encrypt the token descriptor T_2 using the key RK (to obtain $E_{RK}(T_2)$) and to write a number of files onto the disk 46. The application file A (plain text), the encrypted application file $E_{AK}(\text{application file } B)$, the software decryption key $E_{CSK}(AK)$ (prepared if need be as previously described) and the encrypted token data $E_{AK}(T_2)$. Thus at the conclusion of the steps shown in Fig. 7, the disk 46 of the transfer set is substantially identical to the original disk 16 which the user had acquired. The differences are that the token data (which exists in encrypted form) is different on the disks 46 and 16 and if the conditions of execution (such as count) have changed a new encrypted application key file $E_{CSK}(AK)$ has been used. This file is associated with the new token through the synchronous mechanism described previously. Transfer is thus made useless as a piracy method. Of course in installing the right to execute on the coprocessor 20, the user had used (and hence invalidated) his token containing the token data T_1 , and as a result the file set on the original disk 16 is not usable to install a right to execute in another coprocessor. However, the disk 46 includes the encrypted token data corresponding to the token 40 which is now in the user's possession. Accordingly, the user is now in a position to install the right to execute the protected application on another coprocessor; note at the same time that the original coprocessor which previously stored the software decryption key AK , no longer stores that key. Accordingly, the right to execute the protected application has been transferred from the coprocessor 20 to the portable form represented by the distribution set including the cartridge 40 and the disk 46.

While the transfer set including the disk 46 and the cartridge 40 could be used to install the right to execute the protected application on a different coprocessor, it is also usable as a form of external storage for the right to execute, e.g. the user could if he wished install the right to execute back into the coprocessor 20 from which it was derived in the first place.

The direct transfer, from coprocessor to coprocessor, of a right to execute is shown in Figs. 20 and 21. Fig. 20 shows that a source composite processor includes a host 10 and coprocessor 20, a sink composite processor includes a sink host 110 and a sink coprocessor 120. As shown in Fig. 20, the source coprocessor includes the right to execute (AK) which is to be transferred. In general, both coprocessors 20 and 120 would contain the same collection of supervisor keys (CSK); for generality purposes Fig. 20 shows that the source coprocessor will, in the following process, employ

the supervisor key $CSK1$, whereas the sink coprocessor 120 will employ a different supervisor key, $CSK2$. Neither coprocessor has a priori knowledge of which supervisor key is employed by the other. The source and sink processors are interconnected via a communication link 200.

As already described, once communication is established, the coprocessors begin an identifier sequence to ensure themselves that the other is a "member of the family". In step 1 of Fig. 1 outlining this process, each coprocessor generates a random number, so that the source coprocessor generates $RN1$ and the sink coprocessor generates $RN2$. In step 2 each of the random numbers are encrypted under a supervisor key independently chosen by the generating coprocessor and the encrypted information is transferred, so that in step 3 the sink coprocessor 120 has access to $E_{CSK1}(RN1)$ and the source coprocessor has access to $E_{CSK2}(RN2)$. As previously explained, only "members of the family" are capable of decrypting and recognizing the random numbers transmitted thereto. Assuming that the source and sink coprocessors are "members of the family", then each can decrypt the transmitted message so that thereafter both coprocessors have available $RN1$ and $RN2$. As already indicated, the session key SK is a composite of both the random numbers, and in step 4 of Fig. 21 each coprocessor independently determines the identical session key SK .

Thereafter, after the user has identified the right to execute which is to be transferred (AK), the source coprocessor encrypts the right to execute under the session key SK and transmits it to the sink coprocessor (step 5). At this point while the sink coprocessor 120 has access to the right to execute, AK , it is not yet effective. This lack of effectiveness is enforced by the trusted safe procedures imposed on each of the coprocessors. The sink coprocessor returns a message to the source (step 6) indicating receipt of the right to execute. Consequently the source coprocessor can delete the right to execute (step 7). Finally, the source coprocessor (step 8) transmits a message to the sink coprocessor that the right to execute has been deleted. Only thereafter, in step 9, does the sink coprocessor activate the right to execute.

Having described direct transfer of a right-to-execute, or a collection of rights-to-execute it is a simple extension to describe safe procedures for a library type of software distribution among computers in a network. For the reasons already given protected software can only be distributed to composite computing system as heretofore described, i.e. each consists of a host (for example a PC) and a coprocessor. It should be clearly understood that protection is preserved even if some of the participants in the network are not composite computing

systems as previously described. The only consequence of the existence of such interlopers is that the protected software is simply unavailable to them. In such a network any pair of such composite computing systems can safely transfer right(s)-to-execute by the procedures already described. The fact that transfers may be observed (and copied) is of no moment for the reasons already given. One observing a transfer of a right-to-execute would merely observe encrypted messages passing back and forth; without access to the supervisor or session keys protection is preserved by the inability to decrypt or read any of the messages. In such a network there may exist one or more software sources in the sense that a source has available many right(s)-to-execute, including, typically, multiple rights for a single protected application. Clearly such a source may transfer a right-to-execute (assuming that the software flag allows transfer) to many other composite computing systems. Each time a right-to-execute is transferred the source's collection of rights is reduced by the transferred right, and each time a right is returned the source's collection of rights is augmented by that return. The permanent memory of any source always retains a count of available rights and at any time transfer of one or all of the available rights can be effected. It should also be apparent that a source may condition a transferred right, such as for example requiring the transferee user have an account which is charged for the transfer. The transferred right could also be conditioned in terms of time or number of uses, etc. In some cases, for example if a transferred right is conditioned to expire on a date in the future then the source may be arranged to increment its collection of rights-to-execute on passing of the date in an implied transfer transaction. In other words since the transferred right was conditioned to expire on the specified date it is quite appropriate for the source to "reacquire" the previously transferred right after the specified date even though no actual transfer took place. A source may also retain a count of available rights measured by the number of executions, and of course such a source could transfer all or a part of such collection in one or many transactions. Some of those rights could also be returned to augment the source's collection.

In any transfer transaction the only necessary data actually transferred from coprocessor to coprocessor is the encrypted key (and associated flags and conditions); the protected software itself, both encrypted and plain text portions, can be transferred by any conventional means. If efficient, all composite computing systems could have pre-existing access to all (or less than all) of the protected software (in encrypted form) so only the key need be transferred. Software which must be

transferred could be transferred through the same network by which the keys are transferred or the software could be transferred through another network such as the postal service.

Backup the Right to Execute

In the following description, reference is repeatedly made to "reading" a token; the structure of the hardware cartridge storing the token, and the manner in which it is read is described more fully in [YO985-091], [YO986-010], the disclosure of which is incorporated by this reference.

Because the entire backup sequence refers to a failed coprocessor and installs the right to execute on a different coprocessor, we will refer to the failed coprocessor as the source coprocessor and the different coprocessor as the sink coprocessor.

It should already be clear that the right to execute, in the form of a software decryption key AK is stored in the (source) coprocessor 20.

While the coprocessor 20 has features which make it unique, it is similar in at least one respect to any other processor, i.e. it is capable of a failure. With current software distribution techniques, when a user has a processor failure, that failure interrupts his ability to execute software, but that ability can be reacquired by repairing or replacing the failed processor. In the case of the coprocessor 20, however, failure of the device may well permanently impair the right to execute which had been stored therein. Accordingly, software vendors may desire to provide their customers with a "hardware" backup of their rights-to-execute. The "hardware" backup which will be described herein is arranged to minimally impact the security of the right-to-execute, e.g., limit the number and duration of any spurious or duplicate rights to execute. The "hardware" backup to be described can be conceptualized as a pending or inchoate transfer of rights. Because the necessity for the backup depends on a future and uncertain event, e.g. failure of the coprocessor 20, it must be arranged so that the inchoate right to execute can be converted to an actual and usable right to execute entirely independent of the processor 20. For this reason, it does have the feature of generating a duplicate right to execute which could be used by the unscrupulous to thwart the protection sought by the software vendor. However, as will be described, the installation of a backup can only be performed once for any (source) processor and produces a conditioned right to execute, conditioned on a grace period (typically measured from the time of the backup installation). At the conclusion of the grace period, in the absence of further action, the

rights to execute derived from the backup rights are no longer effective. The cost of this severely limited piracy to the unscrupulous is the sacrifice of the possibility of reclaiming that collection of rights to execute in the event of a real coprocessor failure. In the case of a scrupulous user, in the interim, the user is obligated to "prove" to a trusted observer, such as the hardware vendor, that his coprocessor indeed has failed. Typically, this "proof" is effected by physically transmitting the failed coprocessor to the hardware vendor. On review of the failed coprocessor, the hardware vendor will provide to the user a verification disk. The verification disk can be used by the user to provide validated authorization to the (sink) coprocessor to eliminate the condition on the backup rights to execute and convert them into rights to execute conditioned only by the condition set at the time of their acquisition. To ensure that the verification disk is prepared based on evidence of the failure of a coprocessor which is identical to the coprocessor which originally stored the right to execute being replaced, the verification disk carries, in encrypted form, a unique identifier of the failed coprocessor. This unique identifier is necessary to allow the removal of the condition. It is also to be desired that the sink processor be able to recognize that the message to remove the condition from the installed set of rights to execute is intended to be received by it. This is accomplished by including in the message a copy of the (sink) coprocessor's unique key to serve as validation of the message or by encrypting the message with the sink coprocessor's unique key. Both the source and sink processor identifiers are made available to the hardware vendor in an encrypted (under CSK) message prepared by the sink processor to be returned with the failed source processor.

The procedure as just outlined is graphically illustrated, as a function of time which proceeds left to right, in Fig. 17. Initially, coprocessor 20 includes a set of rights to execute. A CBS procedure (create backup set) is initiated; this creates a backup set including a cartridge and a disk. Although this backup set bears some similarity to the transfer set, as will be described below, the CBS procedure is preferably carried out each time the user acquires a new right to execute, so that the single backup set provides a backup for every right to execute within the repertoire of the coprocessor or at least a backup right for each application for which backup is authorized by the software vendor. Fig. 17 also shows that subsequent to execution of the CBS procedure, the coprocessor 20 fails. Thereafter, the user effects an install backup set (IBS) procedure at a time T_s . Accordingly, subsequent to time T_s , the user can employ his rights to execute on the coprocessor 120 in lieu of the failed

coprocessor 20. During that time the user can transmit the failed coprocessor 20 to the vendor who creates a verification disk as a message to the sink coprocessor 120. So long as the user receives the verification disk prior to the expiration of the grace period, he completes the install backup set procedure using the verification disk so as to remove the conditional nature of the rights to execute in the coprocessor 120 (at time T_e).

Referring now to Fig. 8, the coprocessor 20 has a collection of rights to execute represented by the software decryption keys AK_1 and AK_2 . It is these rights which need to be backed up. The first step (Fig. 9) in the backup procedure is for the user to acquire an unused backup set consisting of token 50 and the disk 56. The token includes token data T_B which, for illustration purposes, is shown to consist of a number of portions, T_{B1} , T_{B2} , and so on through T_{Bn} . The disk 56 includes the token data encrypted under the key CSK. The user effects a reading of the disk and by the appropriate utility procedure on the host 10 the coprocessor 20 decrypts the encrypted file read from the disk 56 so that it can store T_B in its temporary memory. At this time, (Fig. 10) the user couples the token 50 to the host 10 via the cartridge connector 18. The coprocessor 20 selects the amount of the token data for use; for this description we assume that the portion T_{B1} is selected for use. The coprocessor 20 generates a random number RN and computes a function of T_{B1} and RN, denominated CR, the computed response of the token. The coprocessor 20 causes the random number RN to be applied to the token 50 to "read" destructively the first portion T_{B1} . Reading this portion of the token 50 destroys the portion T_{B1} and returns to the coprocessor 20 the actual response AR.

Fig. 11 shows the apparatus in the configuration, e.g. the token 50 no longer stores T_{B1} and the temporary memory includes the actual response AR.

At this point the coprocessor 20 compares AR and CR. If they do not correspond, an error condition has been detected, the token 50 is considered unauthentic and the backup procedure terminates. On the other hand, assuming that AR and CR correspond, then the coprocessor 20 accepts the token 50 as authentic and is allowed to proceed further in the backup sequence. Fig. 12 shows that the host 10, via prompting from the coprocessor 20 has generated a new random number for use as a key (RK) and has written the disk 56 to include a number of files. The first mentioned file is merely the encrypted (under RK) version of the token data as modified by the reading operation required to verify the authenticity of the token 15, e.g. the token data T_B has been modified by deleting the portion T_{B1} prior to encryption. The second file

created on the disk 56 by the coprocessor 20 is the encrypted version of the random key used to encrypt the token data. The third file is a copy of the AKs and their individual associated flags and conditions encrypted under the key provided in encrypted form in the second file. This file also contains a copy of the unique supervisor key (USK source) which identifies the source processor. At a later time, as will be described below, in the verification process, the verification disk will identify the coprocessor whose failure has been evidenced to the vendor. The verification process will proceed to remove the expiration condition on the set of rights to execute which have been installed if and only if the verification has correctly identified both the source and sink processors. The resemblance in structure and function of this set of files and hardware to those in the acquire right to execute or transfer transactions should be obvious. At this point, it suffices to note that the user has a backup set token 50 and disk 56 in which the clear text token data in the token corresponds to the encrypted token data in the disk 56. These devices are sufficient to allow a user to install the rights to execute AK₁ and AK₂ on any coprocessor; because the procedure used to install these rights is an IBS, the set of rights to execute when installed will be conditioned by the grace period.

If, subsequent to creating the backup set shown in Fig. 12, the user obtains a right to execute another application, application 3, and installs that right to execute AK₃ in the coprocessor 20, he can employ the backup set to create a backup set encompassing not only AK₁ and AK₂, but also AK₃. In that event the user presents the disk 56 to the composite computing system wherein the encrypted token data is read. The user then performs the steps already described with relation to Figs. 9-12. In the course of this process, the token portion TB2 will be destroyed in verifying the token; thereafter the resulting token data will consist of TB3 . . . TB_n, the encrypted token descriptor file on the disk 56 will correspond and the disk 56 will include the encrypted version of AK₃. If the user had made copies of disk 56 prior to this point, these disks would now be useless for either CBS or IBS transactions as the encrypted token descriptor and RK on these disks would not correctly validate the backup token.

Of course, the user can continue using the backup set consisting of the token 50 and the disk 56 until there is only a single token descriptor portion left in the token 50. At this point, a new backup is required if another CBS is to be performed. The last portion of the backup token may be read by the coprocessor to invalidate the old backup, and a new backup set may be started.

In the event the coprocessor 20 fails, the user

can employ the backup set consisting of the token 50 and the disk 56 in an Install Backup Set (IBS) procedure which is described below, beginning with reference to Fig. 13.

As shown in Fig. 13, the user has presented the backup set to a different composite computing system consisting of a host 110 and a coprocessor 120; it is not at all essential that the host 110 be different from the host 10 in the original composite computing system, it is only necessary that the coprocessor 120 be different from the failed coprocessor 20. As shown in Fig. 13, the coprocessor 120 does not contain any rights to execute in its permanent memory. When the user presents the disk 56, the encrypted random key E_{CSK} (RK) is read and decrypted so that the encrypted token data E_{RK}(TB2 + TB3 . . . TB_n) can be read from the disk and decrypted as shown in Fig. 14. The temporary memory now includes that token descriptor in plain text form. The coprocessor 120 then generates another random number, SRN, and computes a function of a selection portion (TB2) of the clear text token data and the random number SRN; denominated as CR. The coprocessor 120 then interrogates the token and in doing so destroys the next portion TB2 and generates an actual response AR. Fig. 14 is a snapshot of the apparatus at this point. The coprocessor 120 then determines if AR and CR correspond. If they do not, then the token 50 is not considered authentic, an error condition is entered and the Install Backup Set procedure is terminated. On the other hand, if AR and CR do correspond, then the Install Backup procedure continues.

In the next step (which is not specifically illustrated), the encrypted file containing AK₁, AK₂ and USK (source) are read from the disk 56, decrypted and stored in the permanent memory along with their individual conditions and an indication that they are all conditioned by the grace period.

The sink coprocessor now prepares a message to the hardware vendor which is encrypted under a supervisor key CSK and is stored on disk by the host. The message contains a copy of the unique supervisor key (USKs) of both the source and sink processors encrypted under a common supervisor key E_{CSK}(USK_{source} and USK_{sink}). This information is used to verify that the failed processor presented to the hardware vendor is the source processor and to prepare a verification message which will only allow that sink processor to relieve the expiration date condition from that source processor's set of rights.

With coprocessor 120 in this condition, the user can execute protected application enabled by AK₁ and AK₂ during the duration of the grace period. The grace period is measured beginning at the performance of the IBS. In the absence of

completing the IBS during the grace period, the rights to execute are suspended but may be reinstated by completing the IBS.

Assuming, however, that the user obtains the appropriate verification disk from the vendor, then the IBS procedure can be completed as shown in Fig. 15. As shown in Fig. 15, the user has presented to the composite computing system the verification disk 66. The verification disk 66 includes a single file encrypted under the unique key of the sink processor which carries within it a copy of the unique supervisor key identifying the source coprocessor ($E_{USK_{sink}}(USK_{source})$), whose failure has been proved to the vendor. The coprocessor 120 reads the verified disk 66 and decrypts the file. The coprocessor 120 can then compare the contents of the verify file with the copy of the source USK it has stored. If they do not correspond, an error condition is detected, and the conditional rights to execute remain conditioned; they will be suspended with the expiration of the grace period. On the other hand, assuming the verify file does correspond in all respects, then the coprocessor 120 is authorized to take the final IBS steps; these delete the conditional nature of the set of rights to execute AK_1 and AK_2 . At the completion of the IBS procedure (Fig. 16), the coprocessor 120 includes rights to execute AK_1 and AK_2 (conditioned only by their conditions at time of source processor backup) in its permanent memory. In this condition it is in an identical condition, as the coprocessor 20 just prior to the time it failed (Fig. 8). Thus the foregoing steps provide for a "hardware" backup for the coprocessor 20 with minimal impact on the security of the software vendor's rights, e.g. unauthorized duplication of the right to execute.

The backup procedures employing a token use the token and the procedures associated with it to validate to any coprocessor to which the set is presented, that it can accept the rights to execute which are represented by the set. When an "intermediate" coprocessor is employed for backup purposes, the token is unnecessary; it is the procedures which govern the coprocessors (and which are beyond the reach of the user) which provide the safety. Thus, in the case of using an "intermediate" coprocessor for backup purposes, the disk 46 is prepared essentially similar to the manner in which it is prepared when a token/disk pair are used except of course that the disk file representing the token data is completely unnecessary. Perhaps the only other difference is that when the backup set was employed, the decryption key is encrypted under a supervisor key; such an arrangement if used without the cautions might allow any coprocessor to whom such a disk was presented to accept the backup. To prevent this, the key under which the decryption key is encryp-

ted is a Session Key, which is generated between the source coprocessor and the "intermediate" coprocessor. The generation of such a Session Key has already been described; the only information stored by the "intermediate coprocessor" is the Session Key, along with an indication that it is associated with a backup. Because the transfer procedures require invalidation of any existing backup, the "intermediate" coprocessor can be assured that if it has the Session Key available, any Install Backup Set procedure is valid. And, as has already been described, the backup set can be installed on a "sink" coprocessor so long as the "intermediate" coprocessor transfers the Session Key to the sink coprocessor.

Encrypt Vendor Key (EVK)

As described herein, the majority of coprocessors will be employed in a user's composite computing system (including, in addition to the coprocessor, the host) for the execution of protected application software. In this setting the coprocessor has the function of storing in a protected fashion rights to execute one or more pieces of software as well as the function of manipulating such right or rights as described above. As is already described, however, that is not the only function of the coprocessor; coprocessors are also required by the software vendor in preparation of the distributable package. While the software vendor could employ any computing system to provide for the encryption of token data and software under his own secret key (AK) in accordance with the software protection mechanism described in copending application [YO985-091], another component of the distributable set is the software decryption key, encrypted under the hardware vendor's key, e.g., $E_{CSK}(AK)$. In order to secure the hardware vendor's key CSK from knowledge by the software vendor, the software vendor can use a coprocessor (which is equipped with the key CSK in secure storage) for this function. It is already described that this service can be used to facilitate a plain text attack on the key CSK.

While we have postulated the use of DES, which is particularly resistant to the plain text attack, by using the procedures described below that resistance can be enhanced. The plain text attack requires the attacker to have access to plain text and cipher text encrypted under the key under attack. By use of the procedures to be described, we deny the attacker access to such information.

Fig. 18 shows a typical coprocessor 220 used in the mode required by the software vendor wherein input is one or more software decryption keys AK_1 , AK_2 , etc., and output is the keys encryp-

ted under the key CSK. Using the convention already established, the coprocessor 220 is physically and logically secure; that security is indicated by the dashed inner boundary. If the coprocessor 220 merely outputs $E_{CSK}(AK)$ for each software decryption key input, it would readily provide an attacker with the data necessary for a chosen plain text attack.

In accordance with this aspect of the invention, however, the coprocessor 20 modifies the decryption key prior to encryption; the modification, however, is one of which all coprocessors are aware, so that all other coprocessors can perform the inverse modification. In general, each software decryption key AK_i is modified by padding it, front and rear. More particularly, as shown in Fig. 18, a suffix recognition flag (RF) typically in the form of a message authentication code (MAC) of known bit length is used along with a prefix random number (RN). Thus, in response to presentation of AK_i , the coprocessor 220 generates $RN_i.AK_i.RF$ (where $.$ indicates concatenation). The coprocessor thereafter encrypts the resulting concatenation of data blocks under some key CSK among the set of CSKs to produce $E_{CSK_i}(RN_i.AK_i.RF)$. It is self-evident from an understanding of the DES that another coprocessor with access to CSK_i can decrypt the result to produce the string $RN_i.AK_i.RF$. Because the decrypting coprocessor has a priori knowledge of the content and bit length of RF as well as the bit length of a software decryption key such as AK_i , it readily follows that the coprocessor can decrypt the message $E_{CSK_i}(RN_i.AK_i.RF)$ with each of the set of CSKs until the RF decrypts correctly. Once the Coprocessor has found the correct CSK and has decrypted the encrypted information it can also segregate and specifically identify AK_i ; the prefix RN_i is merely discarded (unless as stated earlier it is needed to perform some other verification task).

An understanding of DES should also make it apparent that whereas a plain text attack requires knowledge of sets of plain text and encrypted information such as $AK_1, E(AK_1); AK_2, E(AK_2); AK_3, E(AK_3)$; and so on, someone with access to the coprocessor 220 may readily be able to identify the following sets: $AK_1, E_{CSK_1}(RN_1.AK_1.RF); AK_2, E_{CSK_2}(RN_2.AK_2.RF); AK_3, E_{CSK_3}(RN_3.AK_3.RF)$; and so on. This set or sets of plain text and encrypted data is of substantially less assistance to the attacker in attempting to identify the key under which these various strings are encrypted, even with knowledge of the plain text AK_1, AK_2, AK_3 , and so on.

Accordingly, the coprocessor 220, representing all coprocessors employed by software vendors for encrypting their software decryption keys, performs the following Encrypt Vendor Key (EVK) procedure. A utility program signals the coprocessor 220 that

a EVK sequence is about to begin. The coprocessor 220 requests and is given the vendor key AK to be encrypted. The coprocessor 220 generates the random number (RN) and uses it as a prefix to pad the front end of the key AK. The coprocessor 220 also pads the back end, using the recognition flag (RF) as a suffix. The resulting block or string is encrypted under the supervisor key CSK and the result is passed to the host.

This EVK procedure has the property that by properly selecting the recognition flag, a data block can be encrypted under a selected supervisor key, selected by one coprocessor, and the encrypted block can be decrypted by another coprocessor even though the decrypting coprocessor does not have a priori knowledge of which of the supervisor keys has been selected for the encryption, so long as the decrypting coprocessor has access to a set of supervisor keys which includes all possible supervisor keys. This can be accomplished by a number of means including a priori knowledge in both processor, message authentication codes and by selecting, as the recognition flag (RF) the encrypting supervisor key. For example assume that the encrypting coprocessor selects CSK_n for the purpose of encrypting AK_n . By the foregoing procedure, the encrypting coprocessor produces $E_{CSK_n}(RN.AK_n.RF)$. We assume for this purpose that the decrypting coprocessor has access to all CSKs, although it is not aware of which CSK has been selected for the encryption. The decrypting coprocessor begins with CSK_1 , and decrypts the encrypted block, with each decryption key in turn. Each time the block is decrypted, the suffix is compared to the decryption key. When the suffix and the decryption key match, the decrypting coprocessor has identified the encryption key and at the same time has access to AK_n since the block has already been decrypted using the correct decryption key. Similarly, if a priori knowledge is used the expected string must be found in the RF position or if a MAC is used then the MAC must be valid for the AK_n or for $RN.AK_n$.

Throughout the previous description reference has been made to the software decryption key AK. For reasons which are described below, the block referred to as AK may include not only the software decryption key, but several flags, the conditions of which are selected by the software vendor so as to allow or not to allow certain procedures to be performed. For example, a 1-bit flag can be set to either allow or not allow "hardware" backup procedures to be employed. In the event the "hardware" backup flag is set to disallow the backup procedure, then any coprocessor storing that decryption key would limit the backup procedures to exclude that key (and any others so marked). The software vendor may wish to prevent transfer of a software

decryption key once installed. For this purpose, a 1-bit transfer flag may be provided which will either allow or disallow the transfer operation. If a host requests a transfer procedure, that procedure is allowed only if the transfer flag is set to allow the transfer operation. Each of these limitations are to be understood as data provided to the functions provided in each coprocessor. AKs may also contain the aforementioned conditions of execution which are tested by the individual applications.

Fig. 19 is an example of the appearance of a portion of the permanent memory 25 of a typical coprocessor which has been in use for some time and stores a collection of rights to execute. As shown in Fig. 19, the permanent memory 25 includes a record (or entry) for each of a plurality of different keys, CSK1 through CSKn, AK1 through AKn and: MAK1 and MAK2 are illustrated in Fig. 19. Each record includes a number of fields, one of the fields is the key itself. Associated with each key are a number of binary flags, a bit for each of the following: Meta, Condition, Erase, Transfer and Backup. It should be understood that this list is a useful subset of such flags and that the set would almost certainly be extended by one skilled in the art. The binary flag identifies, for example under the first column, whether or not the key is a Meta key and as shown in Fig. 19 only the last two records indicate storage of Meta keys. In the next column (headed "Condition"), a binary 1 indicates that the key is conditioned and as shown in Fig. 19, keys AK3 and AKn are conditioned. The third column (headed "Erase") indicates, by the binary 0, that a erasure of the key is not permitted; this condition apply to each of the supervisor keys as well as to a particular application key AK2. The fourth column, headed "Transfer" indicates, by the binary 1, that all keys except AK1 are authorized for transfer (except for the supervisor keys, the transfer of these keys is not at all necessary nor desirable). The last column under the binary flag portion of Fig. 19 is headed "Backup", and the binary 1 indicates that the associated key is authorized for backup. As shown in Fig. 19, keys AK3 and AKn are not authorized for backup.

The memory depicted in Fig. 19 includes a number of multibyte entries for each of the keys. One of the multibyte entries is headed "Condition" and this field includes the data associated with a conditioned key, and thus keys AK3 and AKn include data in that field which can be tested by criteria stored in the application they decrypt to determine if execution is authorized. The last column in the multibyte entry portion of Fig. 19 provides location and verification information which aid searches for an applications key and verification of the key as the one sought.

Software Return

From the foregoing description it should be apparent that the procedures described for manipulating rights to execute allow the software vendor to institute a software return policy which is fair to his customers as well as to himself. For economic reasons, some vendors may desire to limit the return of software to some fixed period (akin to a warranty) although that has no bearing on the present invention. A software vendor may for example allow the return of software (for full or partial credit at the vendor's selection) by requiring the user to provide the vendor with a transfer set including the right to execute the particular software application package. The manner in which the user can create such a transfer set has already been described. If the user presents to the software vendor a valid transfer set including the particular application package for which return is sought, the software vendor is assured (by the operation of the software copy protection mechanism) that the user himself no longer retains the right to execute that software. As is described above, creation of a transfer set requires deletion of the decryption key from the coprocessor.

It should be apparent from the foregoing that the invention provides wide flexibility for manipulating rights to execute in the software protection mechanism described in copending application [Y0985-091]. The present application describes several of these procedures by describing the logical operations and their interrelation. To generate from the description provided herein, software to execute those logical operations will be apparent to those skilled in the art and hence a specific description of software to implement the procedures which have been described is deemed unnecessary.

The techniques taught herein for the manipulation of rights to execute can be used for more general operations as well; examples are described briefly in the following:

A) A method of identifying companion processors to each other which companion processors are characterized by storing a set of keys, which set includes a number of keys greater than one, comprising the steps of:

a) generating a random number at one processor, concatenating said random number with a message authentication code, to produce a concatenated result and encrypting said concatenated result under one key of said set of keys to produce a first identifier,

b) generating a random number at said other processor, concatenating said random number with a message authentication code, to produce a concatenated result and encrypting said

concatenated result under another key, said another key selected by said other processor from said set of keys, to produce another identifier,

c) transmitting said one and another identifiers to said other and one processors, respectively,

d) verifying, at said processors that said identifiers were generated by companion processors by:

1) decrypting said identifiers with keys selected from said set of keys until a decrypted result includes a valid message authentication code as a portion, or

e) not verifying said processors are companion processors if all keys in said set are employed without any decrypted result including a valid message authentication code.

B) A method of inter-processor communication which restricts exchange of key information to within a class of companion processors which are characterized by storage of a set of keys greater in number than one, said method comprising the steps:

i) using the above-described method of identification,

ii) combining said one and another identifiers at both said processors to produce a session key, and

iii) exchanging key information by first encrypting said key information under said session key and transmitting said encrypted key information from one to said other or from said other to said one processor.

C) A method of safely increasing storage capacity for software keys normally stored within a logically and physically secure finite store accessible to a logically secure coprocessor element of a composite computing system without comprising security of said software keys comprising the steps of:

a) selecting one more software keys for storage external to said logically and physically secure storage to form a key block,

b) generating a random number,

c) encrypting said key block under said random number to produce an encrypted key block,

d) storing said random number internally to said physically and logically secure coprocessor,

e) storing said encrypted key block external to said physically and logically secure coprocessor in otherwise unsecured storage, and

f) erasing said software keys from storage internal to said logically and physically secure coprocessor.

D) A method of storing and retrieving a set of software keys stored external to a physically and logically secure coprocessor element of a compos-

ite computing system without comprising security of any of said set of software keys, wherein said coprocessor has access to a set of supervisor keys, said method comprising the steps of:

i) storing said software keys as recited in claim 18,

ii) retrieving said encrypted key block and said encrypted key from said external storage,

iii) decrypting said encrypted key with a selected one of said supervisor key and verifying the presence of a valid message authentication code,

iv) repeating step iii) with each different supervisor key until one such step results in a valid message authentication code,

v) decrypting said encrypted key block with that unselected portion of the result of step iv), whereby a result of said step v) is the original key block including each of said selected software keys.

Claims

1. A method of manipulating a right to execute in a logically secure coprocessor (20) associated with a host processor (10), where said coprocessor stores at least a first key (CSK) and a second software key (AK) representing said right to execute a particular application, said host processor having access to said particular application encrypted under said second software key, said method comprising the steps of:

a) providing to the coprocessor a transfer set including at least a writable medium (46) and a physically and logically secure medium (40), said physically and logically secure medium storing clear text token data (T2),

b) providing to said coprocessor a data block (E_{CSK} (T2)) comprising said clear text token data encrypted under said first key,

c) decrypting said data block, in said coprocessor to produce said clear text token data.

2. The method of claim 1 including further steps to safely extract the right to execute:

d) encrypting said clear text token data in said coprocessor under said second software key (AK) to produce a corresponding data block,

e) encrypting said software key under said first key to produce an encrypted software key, and

f) writing said corresponding data block, said encrypted application file and said encrypted software key to said transfer set and deleting said software key from said coprocessor,

whereby said software key is removed from said coprocessor and written to said transfer set.

3. The method of claim 2 including further steps to transfer a right to execute to a different host processor associated with a different coprocessor:

-providing said transfer set to said different coprocessor storing said first key but not said software key, and

- 1) extracting and decrypting said software key,
- 2) extracting said corresponding data block and decrypting said corresponding data block to produce corresponding clear text data,
- 3) reading said physically and logically secure medium to determine whether said clear text token data does or does not correspond to said corresponding clear text data, said reading step necessarily altering said clear text token data is stored in said physically and logically secure medium,
- 4) if said data do not correspond,
 - a) rejecting said transfer, if said data do correspond,
 - b) storing said decrypted software key, whereby said reading step (3) destroys said clear text token data so that no further transfers may be authorized by said physically and logically secure medium.

4. The method of claim 1 including further steps to provide backup for a right to execute:

- d) challenging said physically and logically secure medium (40) to verify that the decrypted token data corresponds to the token data stored by said physically and logically secure medium,
- ei) in the event there is no correspondence, rejecting said backup set and terminating said steps,
- eii) in the event there is correspondence, then
 - f) modifying and then encrypting said decrypted token data under said software key,
 - g) encrypting said software key under said first key, and
 - h) writing results from said steps f) and g) to said backup set, and writing said protected application to said backup set.

5. A method as claimed in claim 4 which includes the further steps of:

- g1) requiring presentation to said coprocessor of any previously written backup set,
- g2) invalidating said backup set, and
- g3) only after executing said step g1) and step g2), if there was any previously written backup set, proceeding to execute said step h).

6. The method as claimed in claims 4 or 5 in which said step d) includes: modifying said token data stored in said physically and logically secure medium so that thereafter said physically and logically secure medium stores modified token data.

7. The method of any claims 4 - 6, including further steps to install the backup set on a different coprocessor:

- k) presenting said backup set to said different coprocessor,

l) passing said encrypted modified token data to said coprocessor and decrypting said token data so that said coprocessor has access to decrypted modified token data,

m) challenging said physically and logically secure medium to verify that the decrypted modified token data corresponds to the modified token data stored by said physically and logically secure medium,

ni) in the event there is no correspondence, rejecting said backup set and terminating said steps,

nii) in the event there is correspondence, then

o) accessing, decrypting and storing in permanent memory of said different coprocessor said software key representing a right to execute said protected application by a user of said different coprocessor, and

p) conditioning said right to execute for use only within a grace period.

8. The method as claimed in any of the claims 4 - 7 in which said challenging step comprises:

- generating and storing a random number in said different coprocessor,
- generating a computed response as a function of both said random number and said decrypted modified token data,
- transmitting said random number to said physically and logically secure medium,
- generating in said physically and logically secure medium an actual response by reading said modified token data as selected by said random number,
- transmitting said actual response to said different coprocessor, and
- comparing said actual response and said computer response.

9. The method of claim 1 including further steps to safely distribute demonstration software:

- distributing said demonstration software on the transfer set in a form in which at least a portion thereof is encrypted under a software key, and along with said demonstration software said software key encrypted under a further key and a null token data file, encrypted under said software key, said software key including at least a condition of use flag inhibiting any coprocessor from erasing said software key, once installed,
- searching said permanent memory to determine if said demonstration software key had previously been installed,
- writing said software key to a permanent memory of said coprocessor only if said searching step indicates that said demonstration key had never been previously installed, whereafter said demonstration software can be executed on said composite computing system by decrypting encrypted por-

tions by said coprocessor, or omitting said writing step in the event said demonstration software key had been previously installed wherefore said demonstration software cannot be executed on said composite computing system, whereby a user may install said demonstration software into a composite computing system only on a single occasion thereby protecting software vendors from users repeatedly installing demonstration software.

10. A method of manipulating a right to execute a particular protected application on a composite computing system including a host processor (10) and a physically and logically secure coprocessor (20), wherein said protected application includes at least a portion encrypted under a software key and said right to execute is represented by said software key stored in a permanent memory of said coprocessor which coprocessor also stores a first key (CSK) in said permanent memory, said method comprising the steps of:

a) coupling said first coprocessor (20) to a second coprocessor (120) for bidirectional communication,

b) challenging said second coprocessor to determine if it is a trusted recipient and simultaneously transferring antecedent information to said second coprocessor to allow access to an encrypted entity,

c) if said second coprocessor is considered a trusted recipient, encrypting said software key under a specific key, derivable by a trusted recipient from said antecedent information, to produce an encrypted software key and transmitting said encrypted entity to said second coprocessor,

d) if said second coprocessor is not considered a trusted recipient then returning an error condition and terminating step c.

11. A method as recited in claim 10 in which said second coprocessor is considered a trusted recipient only if it stores a set of cryptographic keys (CSK1, CSK2..) in common with a set of cryptographic keys stored in said first coprocessor, wherein said step b) comprises:

b1) generating a random number at said first coprocessor, concatenating said random number with a message authentication code to produce a concatenated result and encrypting said concatenated result with a key selected by said first coprocessor from said set,

b2) transmitting a result of step b1) to said second coprocessor corresponding to said antecedent information,

b3) receiving, from said second coprocessor a message and decrypting said message with a key from said set, if a decrypted result includes a valid message authentication code, proceeding to a step

b5), otherwise,

b4) repeating step b3) with each second key in said set until each key in said set is used without producing a result as set forth in step b3), and thereafter proceeding to said step d),

b5) creating a session key by concatenating said random number with the decrypted result of step b3) exclusive of the message authentication code of step b3),

b6) thereafter using said session key as the specific key,

whereby only if said second coprocessor is a trusted recipient will an encrypted software key be transmitted and only the second coprocessor with access to said session key can decrypt said entity to secure access to said software key.

12. A method as recited in claim 11 in which said method includes the following steps performed at said second coprocessor if said second coprocessor is a trusted recipient:

b1a) generating a second random number and selecting a key from said set,

b2a) concatenating said second random number of step b1a) and a message authentication code to produce a concatenated result,

b3a) encrypting said concatenated result of step b2a) to produce said message and transmitting said message to said first coprocessor.

13. A method as recited in claim 12 in which said second coprocessor:

b4a) decrypts information transmitted by said first coprocessor with a key from said set,

b5a) if a decrypted result includes a valid message authentication code, retaining said decrypted result exclusive of the key of step b4a),

b6a) combining said retained result of step b5a) with said second random number to produce said session key,

whereby both said first coprocessor and said second coprocessor have access to said session key without said session key being accessible to any other agency even if all information exchanged by said coprocessors is observed and copied.

14. A method as recited in one of the claims 10 - 13 wherein the encrypted entity is a software key and which comprises, for transferring the right to execute, the further steps of:

e) acknowledging, to said first coprocessor, receipt by said second coprocessor of said encrypted software key,

f) deleting said software key from said first coprocessor and transmitting an indication of said deletion to said second coprocessor, and

g) in response to said indication of said deletion transferring said software key to a permanent memory of said second coprocessor.

15. A method as recited in claim 14 in which said first coprocessor stores said software key in permanent memory along with an indication as to the existence of any backup rights and in which said step c) includes the further steps of:

- c1) checking for existence of an indication of any backup, in the presence of such indication,
- c2) invalidating such backup,
- c3) verifying such invalidation and only thereafter,
- c4) encrypting and transmitting said encrypted software key.

16. The method of one of the claims 10 - 13, wherein the encrypted entity is a backup and which comprises, to install the right to execute on a further processor, the steps of:

- e) accessing, decrypting and storing in permanent memory of said further coprocessor said software key representing a right to execute said protected application by a user of said further coprocessor, and
- f) conditioning said right to execute for use only within a grace period.

17. The method as claimed in any of the claims 1 - 16 which, to encrypt software keys, includes the steps of:

- a) accepting a software key for encryption,
 - b) padding said software key with a number of a given length, said number including at least a component which is random,
 - c) encrypting a result produced by said step
 - d) under said first key,
- whereby said random number padding produces an encrypted result in response to a first encryption operation which is different from an encryption result produced on a second encryption operation even though an identical software key is presented on each occasion thus foiling a plain text attack on said first key.

18. A method of safely transferring a right to execute from a logically secure source coprocessor associated with a host source processor to a logically secure sink coprocessor associated with a host sink processor, where said source coprocessor stores at least a source key and a software key representing said right to execute a particular application and said sink coprocessor stores a sink key, both said source and sink keys includes within a set of keys stored in both said source and sink coprocessors, said host processors having access to said particular application encrypted under said software key, said method comprising the steps of:

- a) generating a random number at said source coprocessor, concatenating said random number with a first message authentication code to produce a concatenated result and encrypting said concatenated result under said source key to produce a source identifier,
- b) generating a random number at said sink

coprocessor, concatenating said random number with a second message authentication code to produce a concatenated result and encrypting said concatenated result under said sink key to produce a sink identifier,

- c) transmitting said source and sink identifiers to said sink and source coprocessors, respectively,
- d) verifying, at said coprocessors that said identifiers were generated by companion coprocessors by

- 1) decrypting said identifiers with keys selected from said set until a decrypted result includes a valid message authentication code as a portion, or
- 2) until all keys in said set are employed without any decryption result including a valid message authentication,

- 3) terminating said method if step d2) is reached, and otherwise,

- e) creating a session key at each coprocessor from said source and sink identifiers,

- f) encrypting said software key at said source coprocessors under said session key to produce a transmittable software key and deleting said software key from said source coprocessor,

- g) transmitting said transmittable software key from said source to said sink coprocessor,

- h) decrypting said transmittable software key at said sink coprocessor with said session key to recreate said software key, and

- i) storing said software key in a non-volatile memory of said sink coprocessor,

- j) erasing said software key from a non-volatile memory of said source coprocessor,

whereby said software key has been extracted and transferred from source to sink coprocessors without exposing said software key outside said coprocessor and without revealing, outside either coprocessor either of said source or sink keys.

FIG. 1

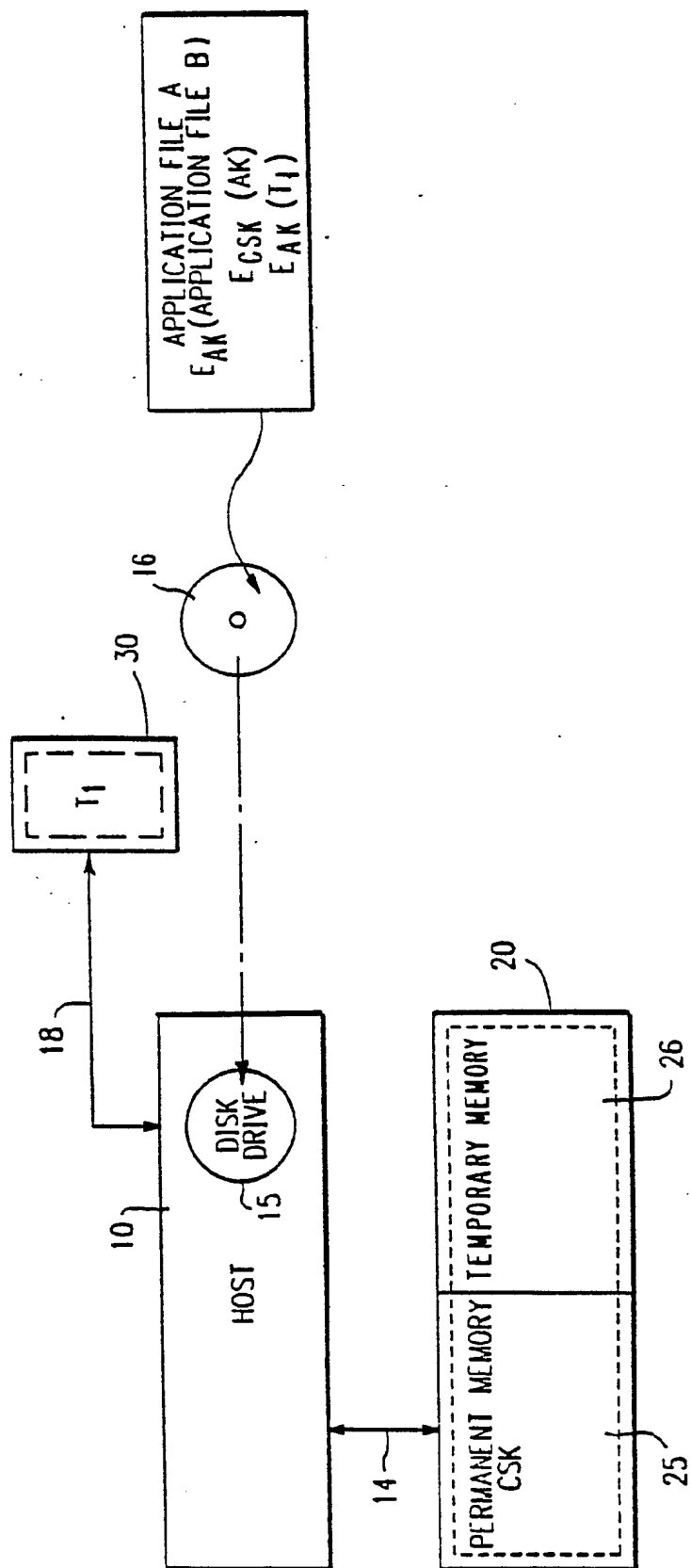


FIG. 2

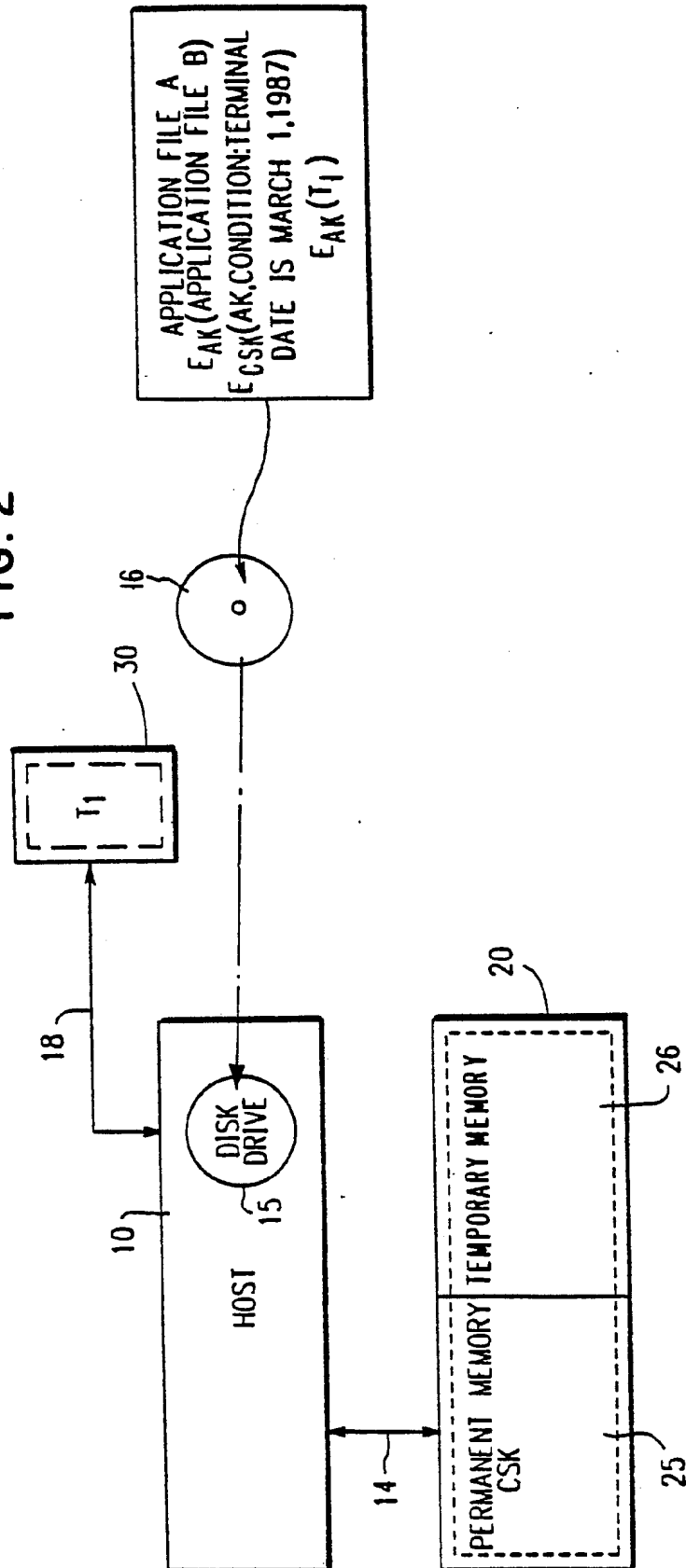


FIG. 3

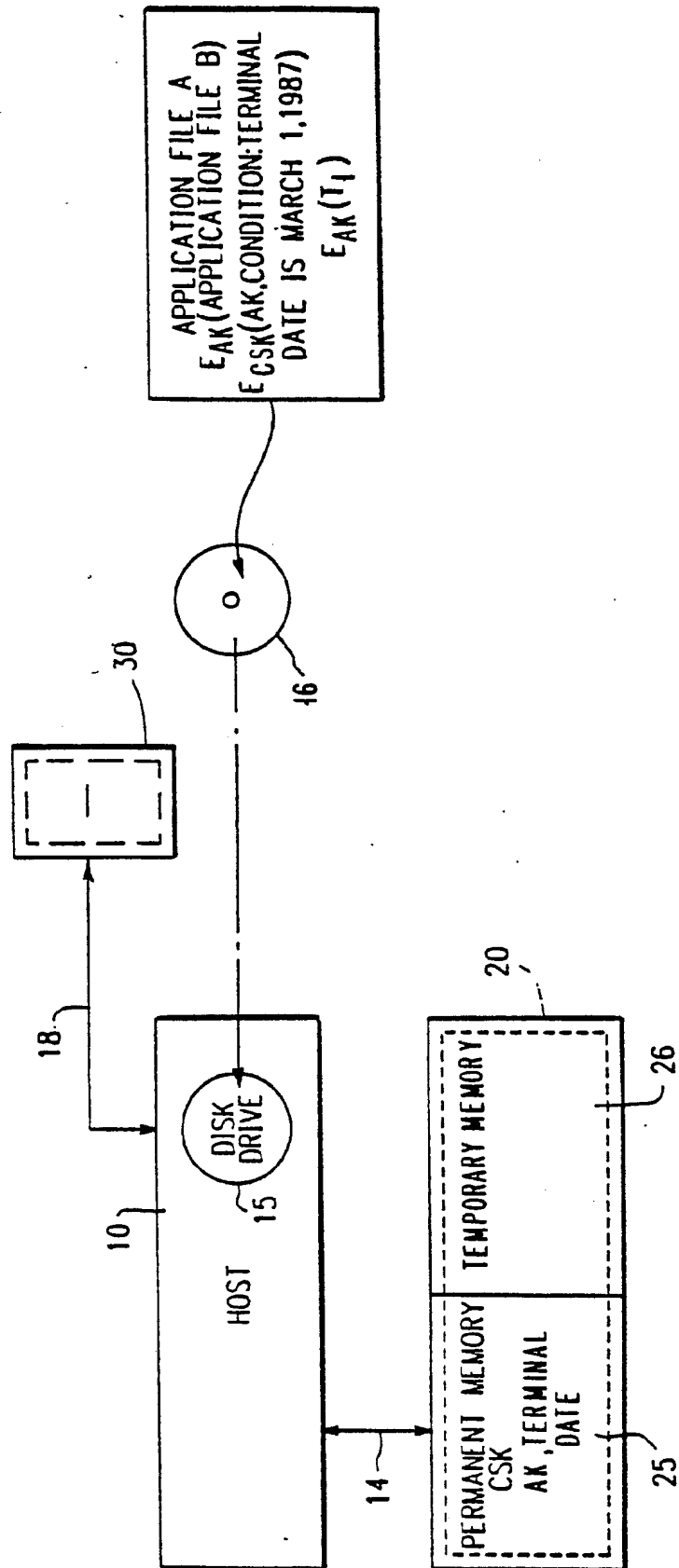


FIG. 4

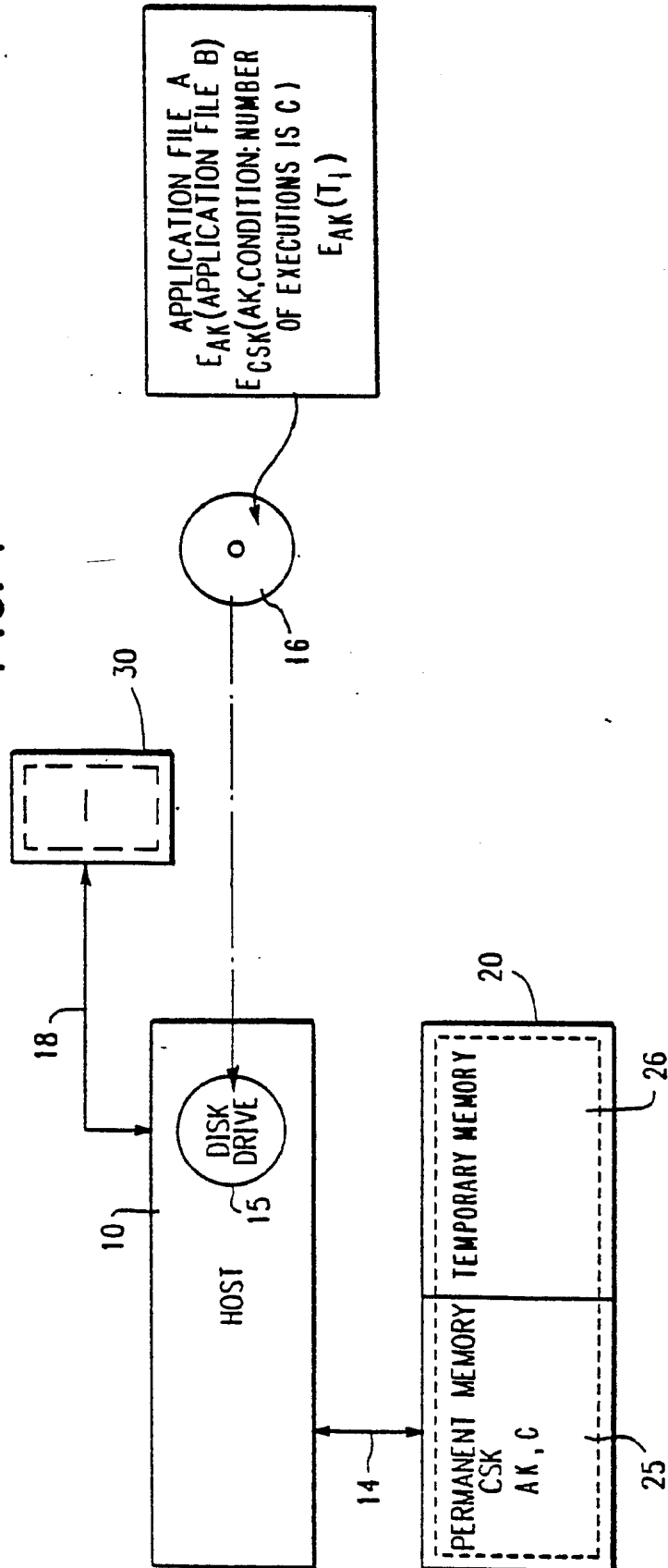


FIG. 5

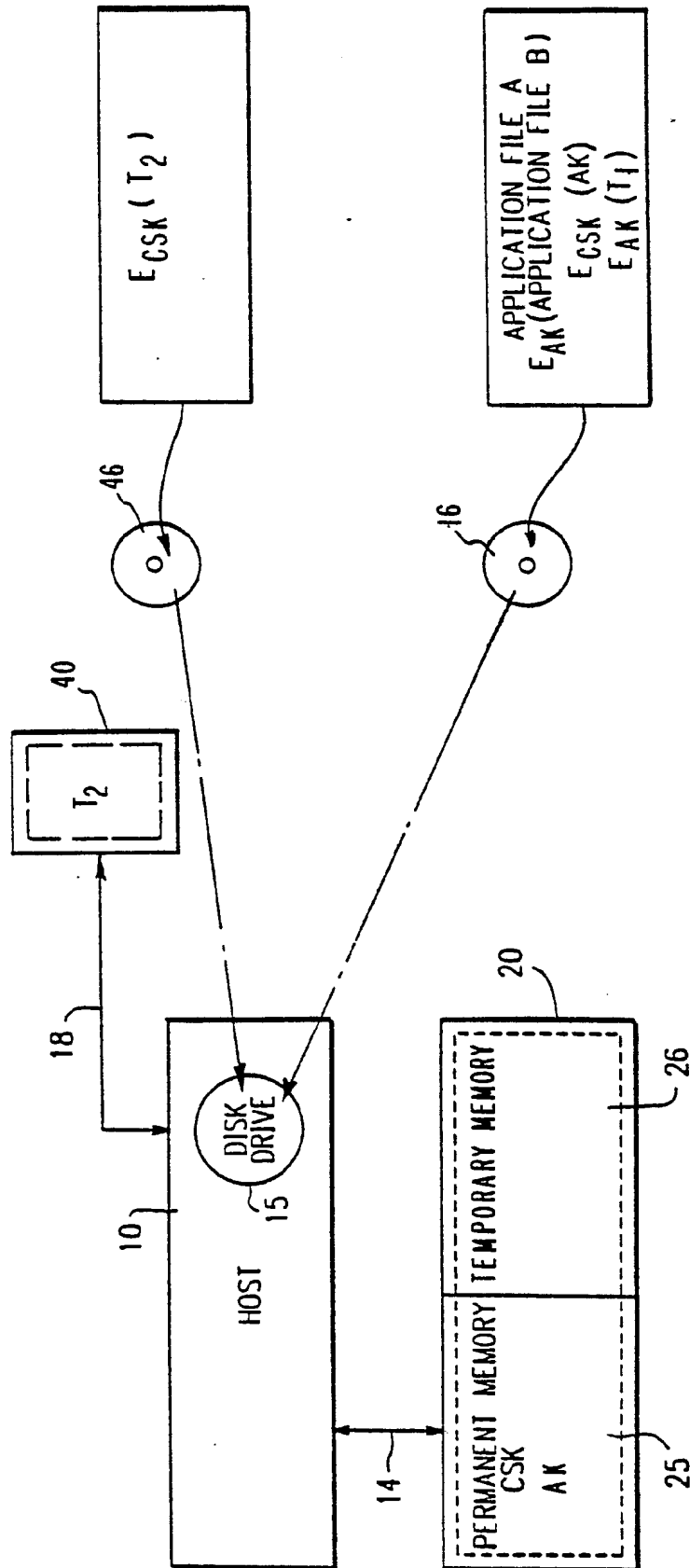


FIG. 6

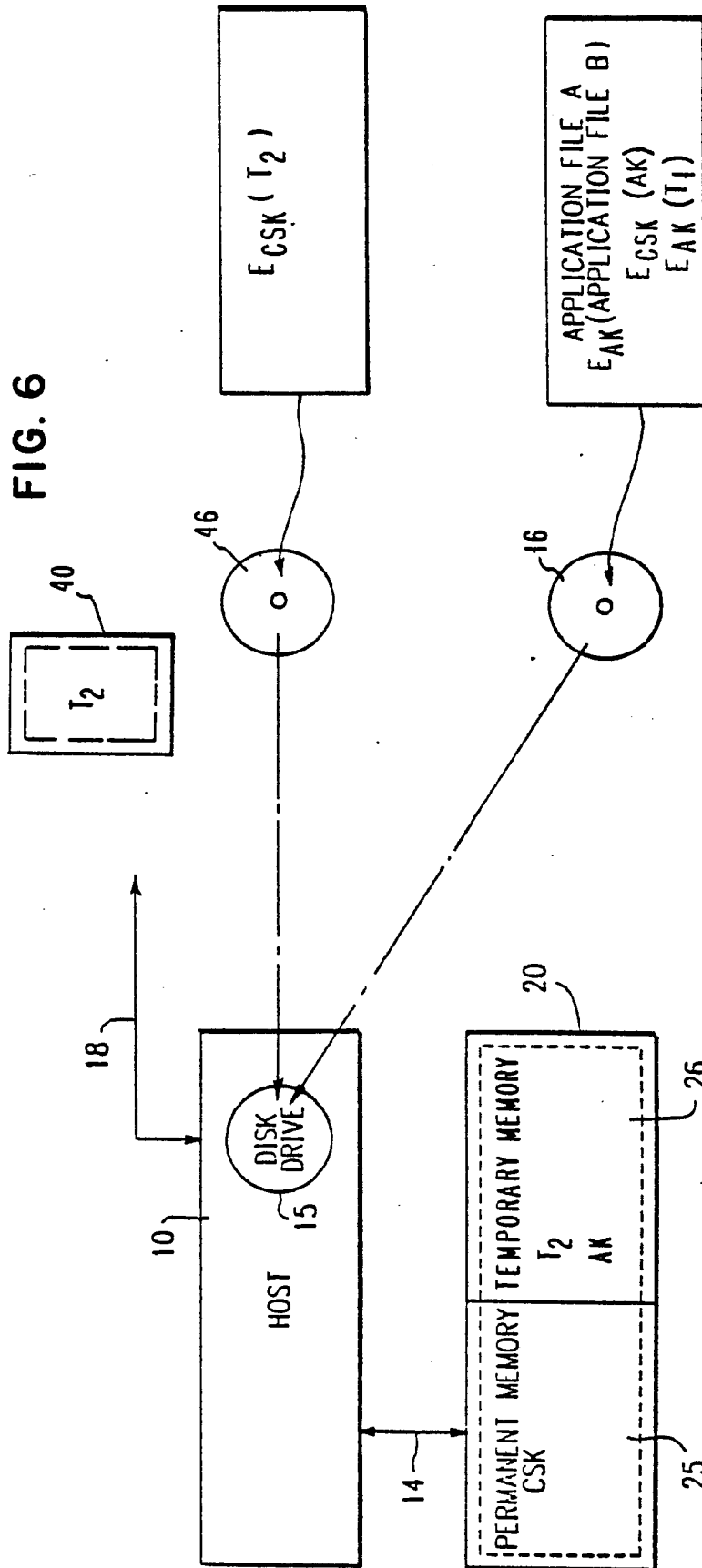
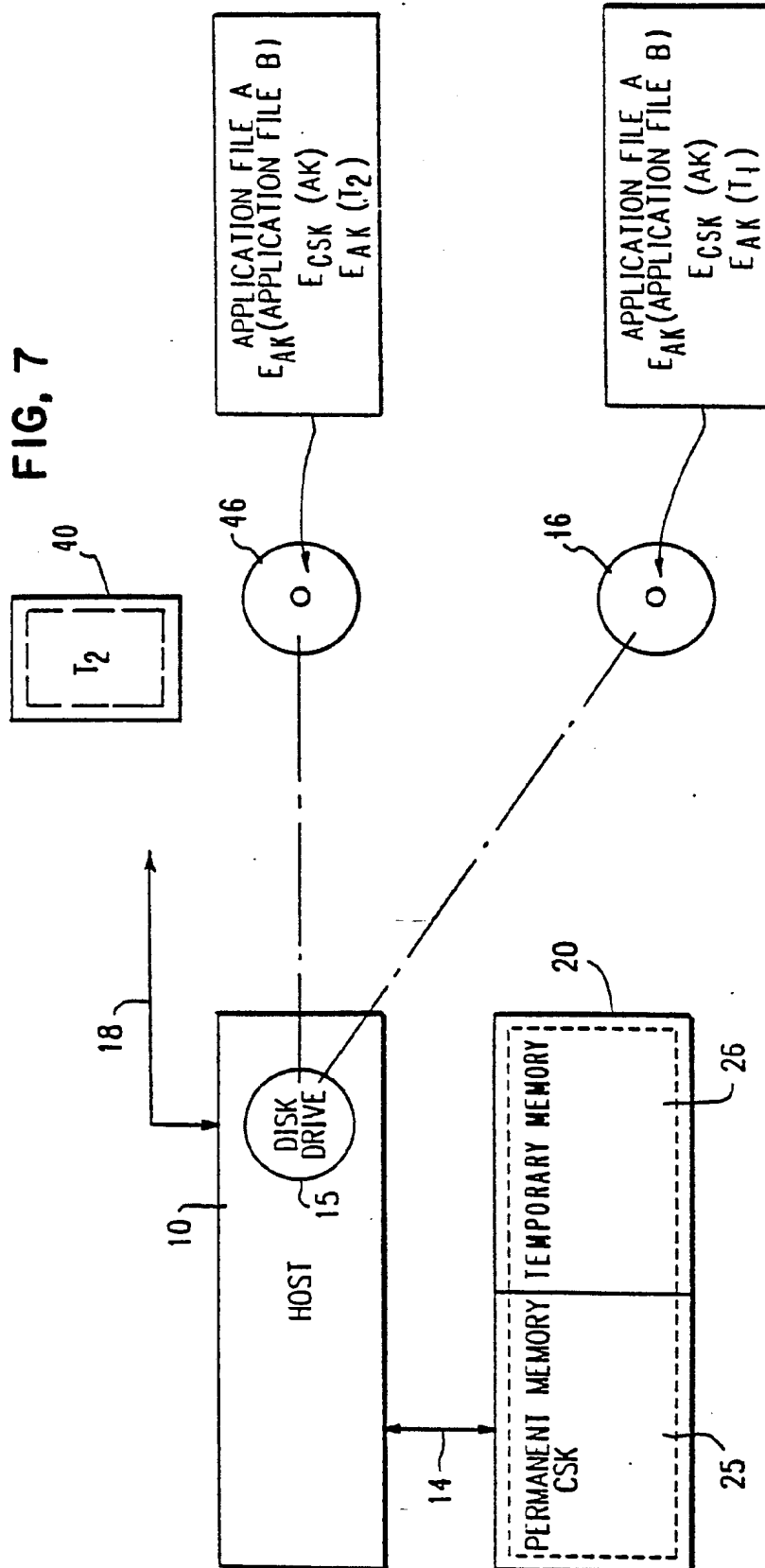
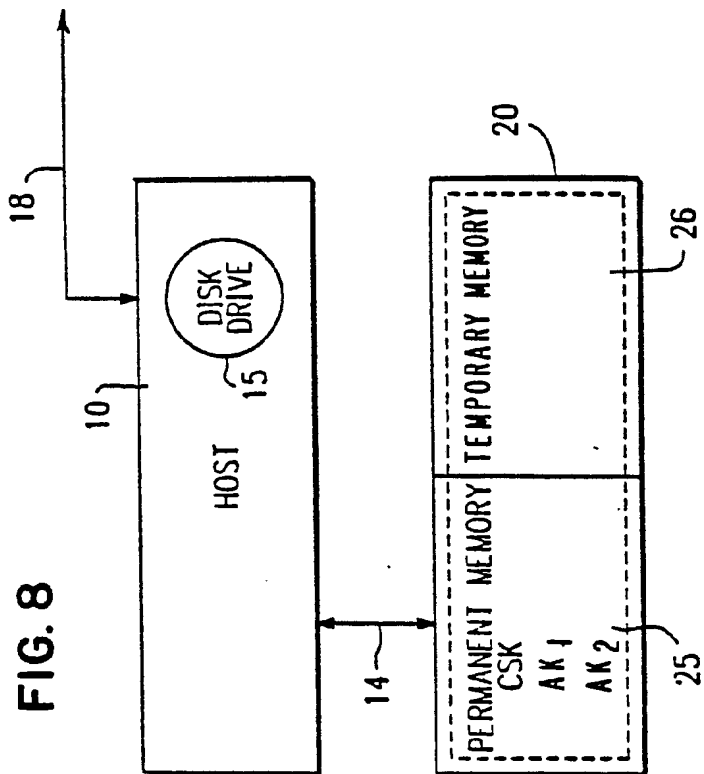


FIG. 7





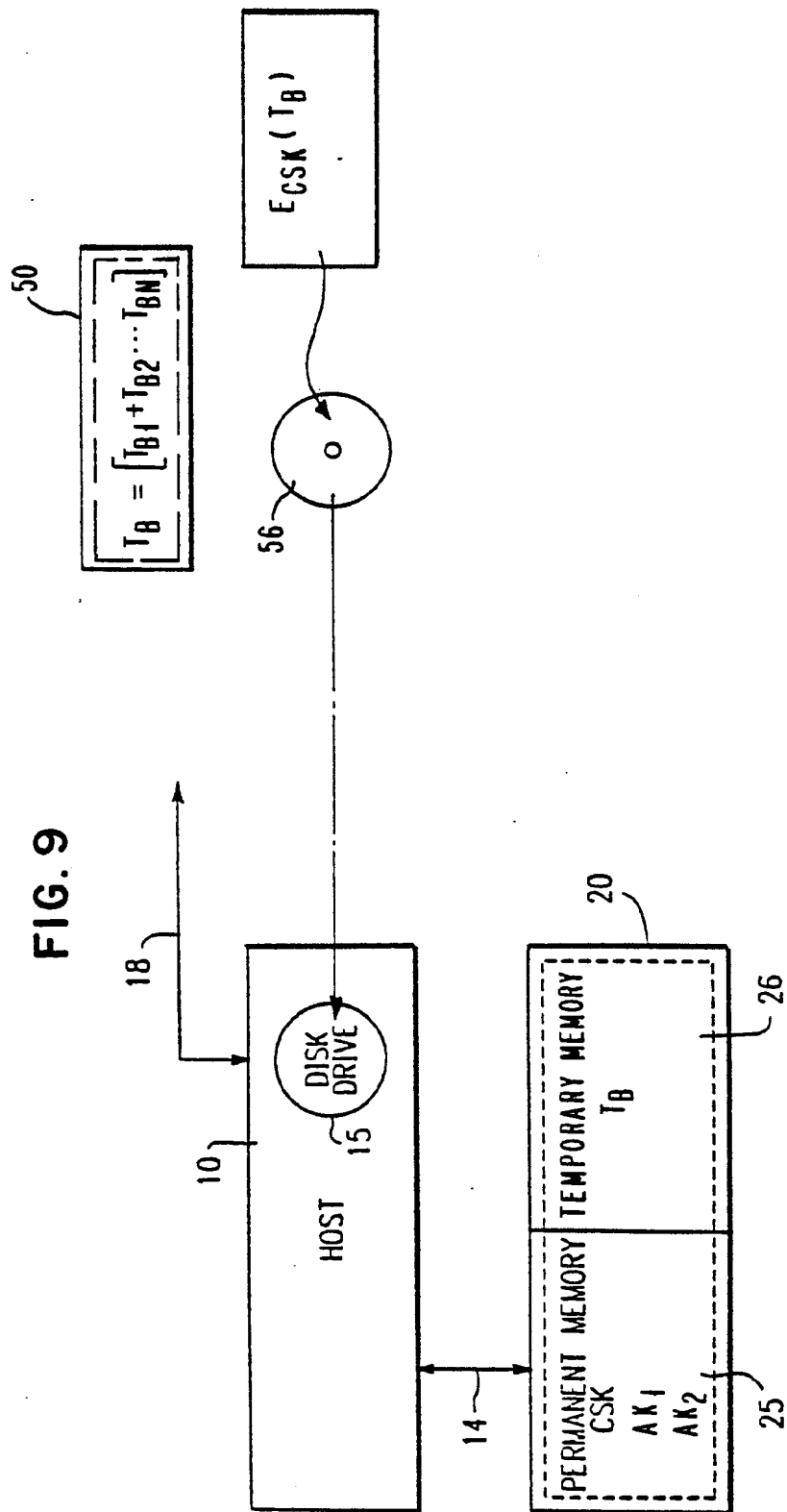


FIG. 10

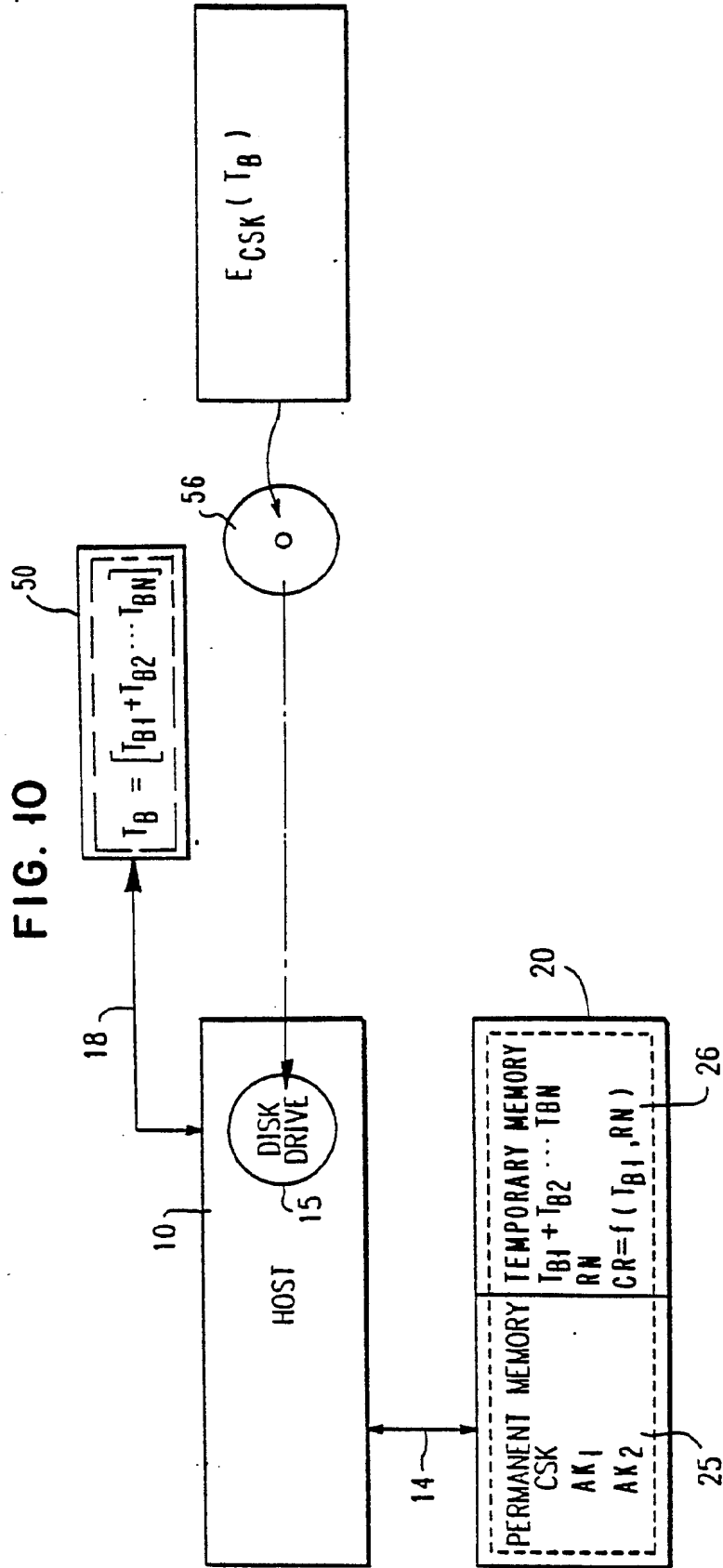


FIG. 11

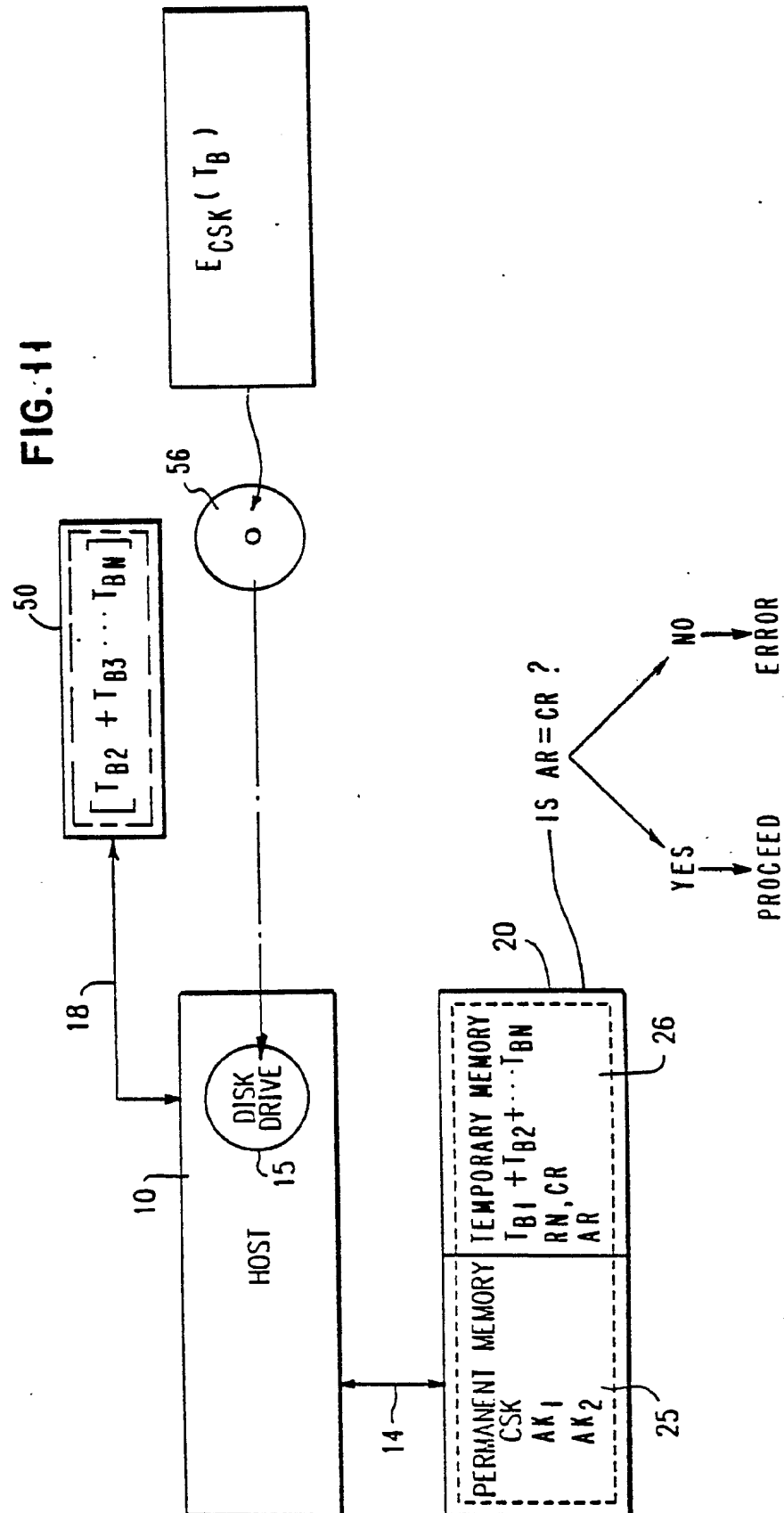


FIG. 12

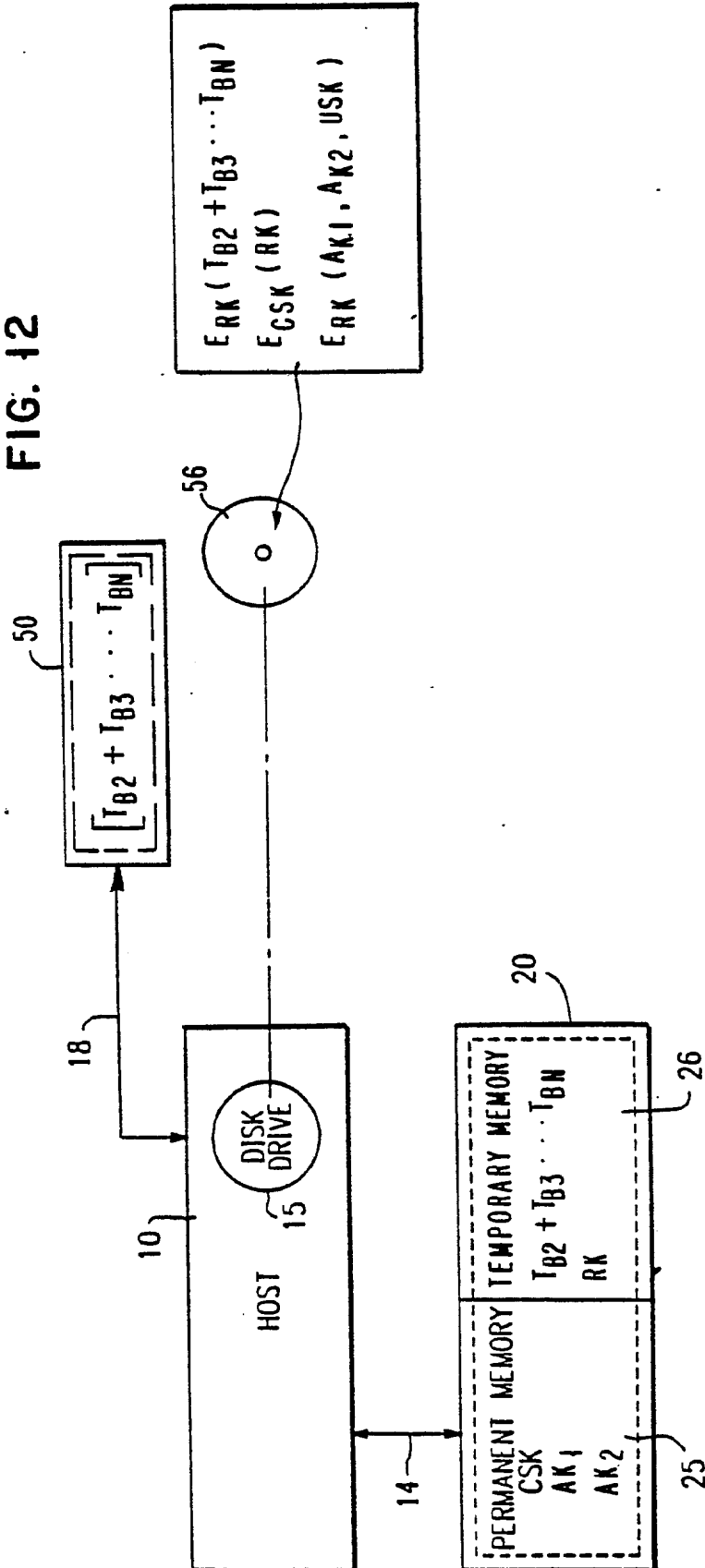
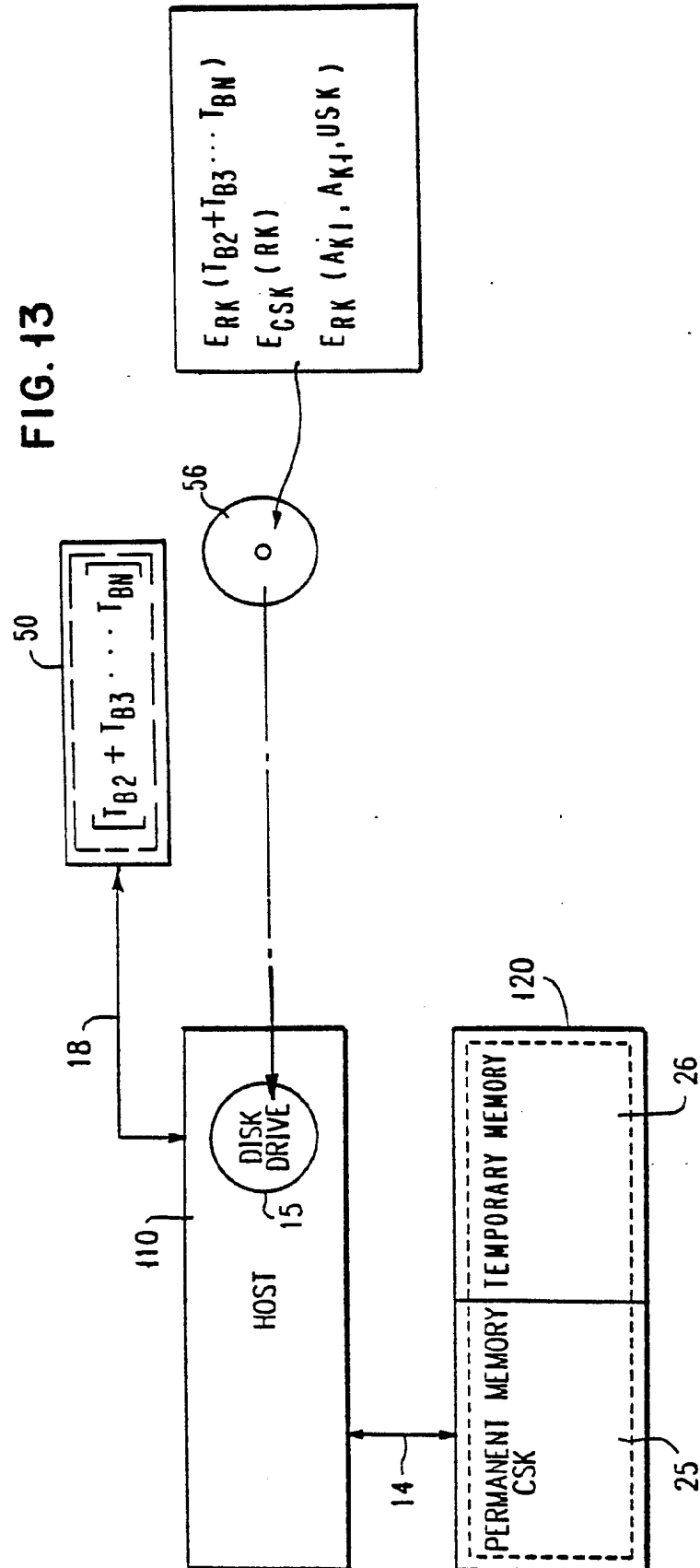


FIG. 13



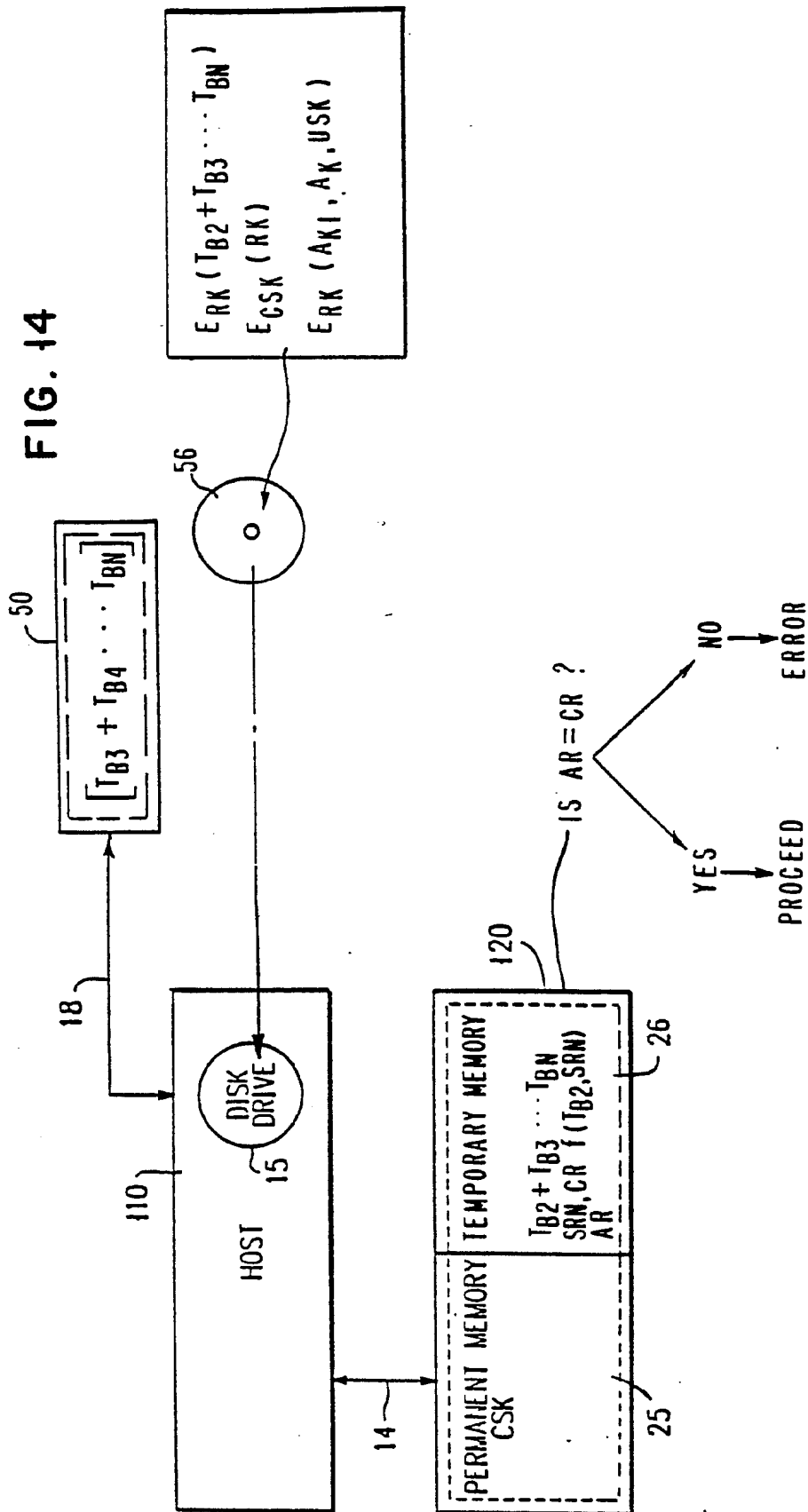


FIG. 15

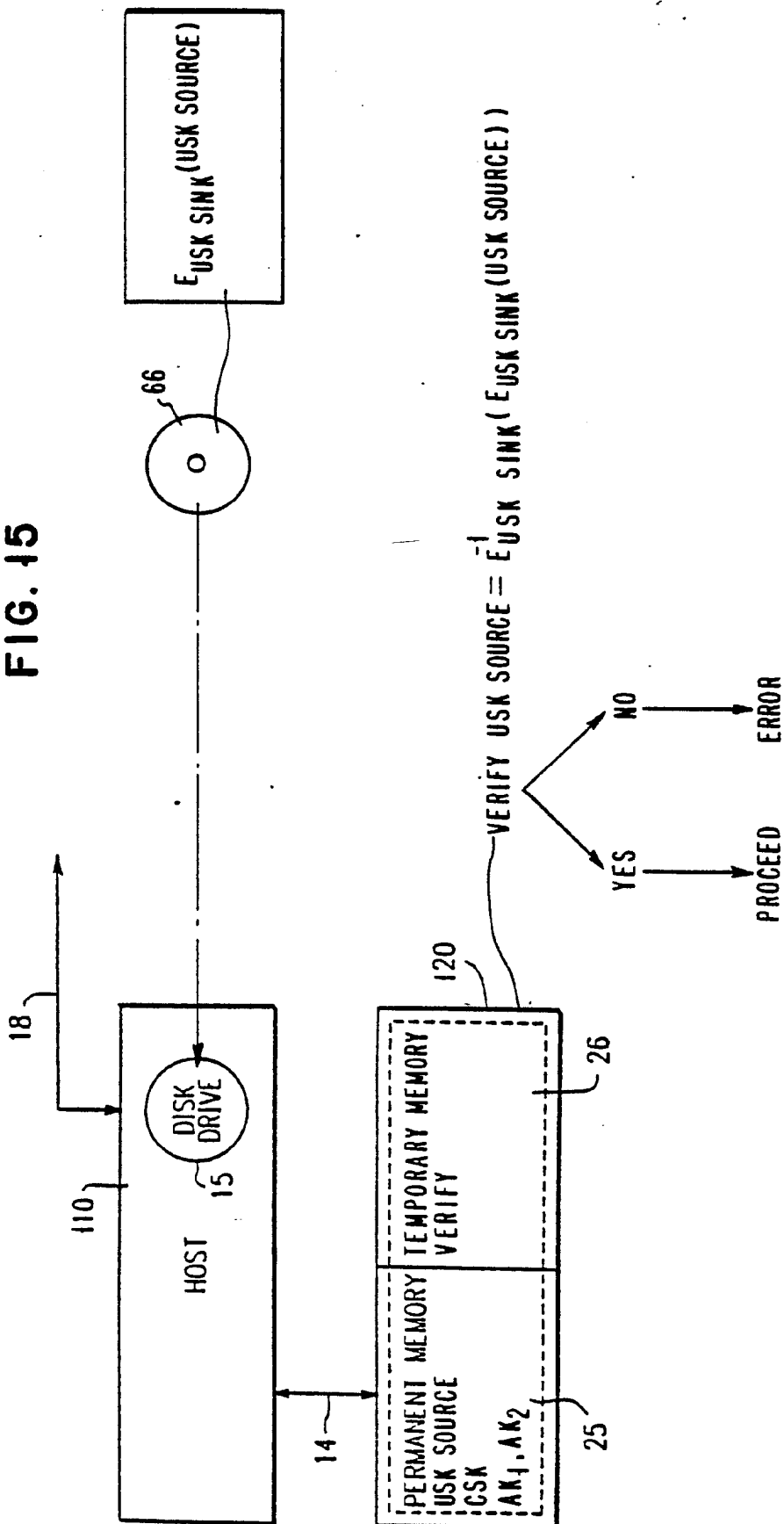
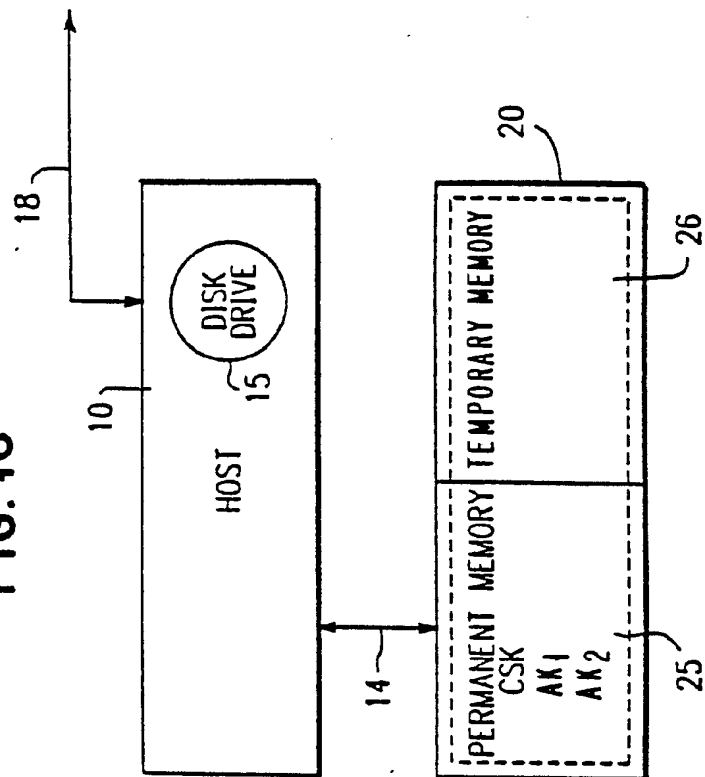


FIG. 16



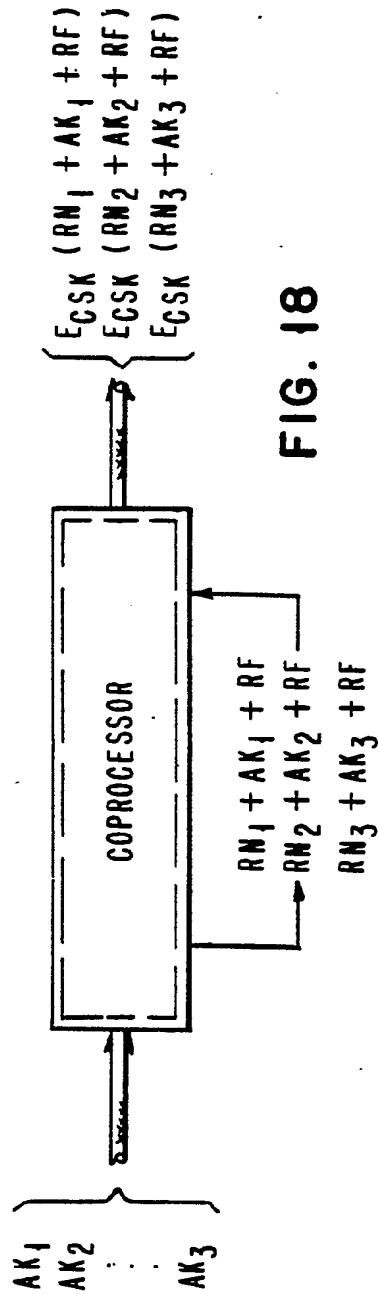


FIG. 18

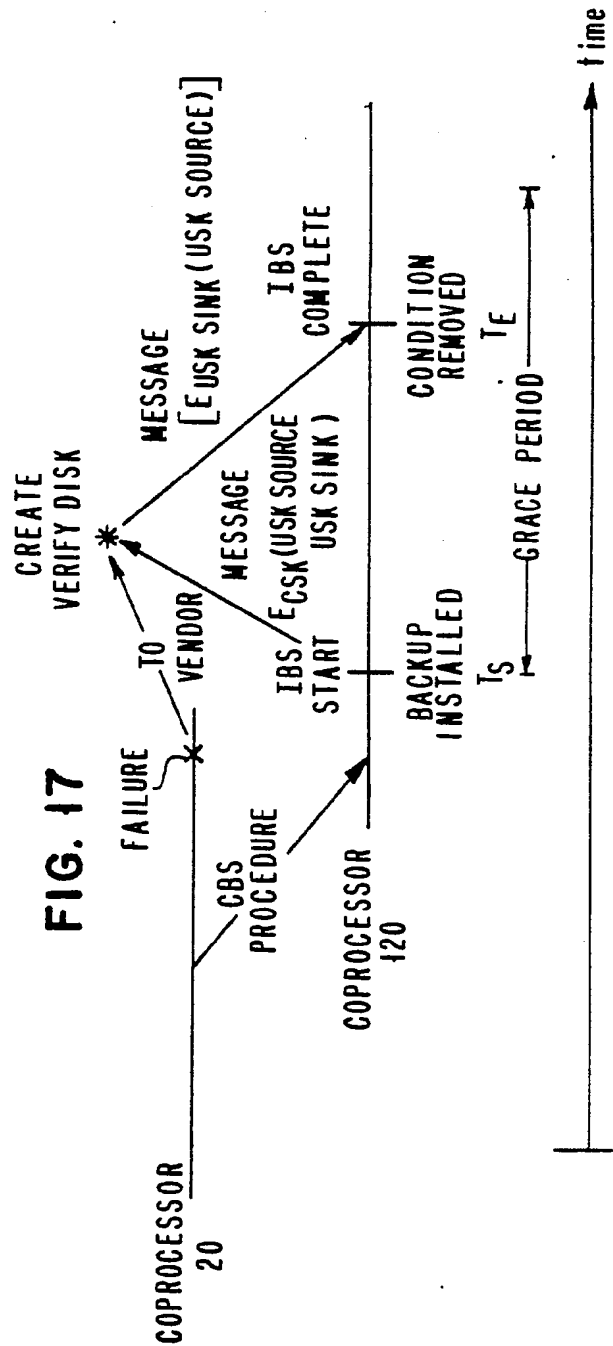


FIG. 17

FIG.19

BINARY FLAGS					MULTI-BYTE ENTRIES		
META	CONDITION	ERASE	TRANSFER	BACKUP	CONDITION	LOCATION AND VERIFICATION INFORMATION	KEY
0	0	0	0	0	_____		CSK 1
0	0	0	0	0	_____		CSK 2
:							:
0	0	0	0	0	_____		CSK N
0	0	1	0	1	_____		AK 1
0	0	0	1	1	_____		AK 2
0	1	1	1	0	DATA		AK 3
:							:
0	1	1	1	0	DATA		AK N
1	0	1	1	1	_____		MAK 1
1	0	1	1	1	_____		MAK 2

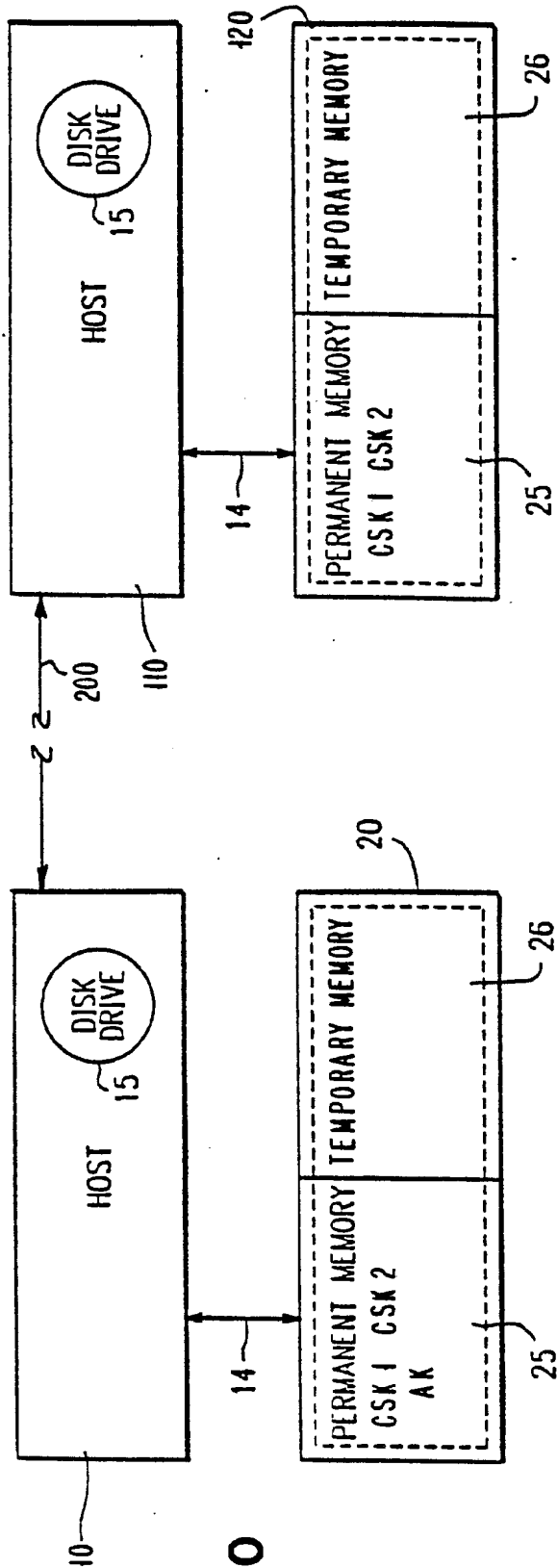


FIG. 20

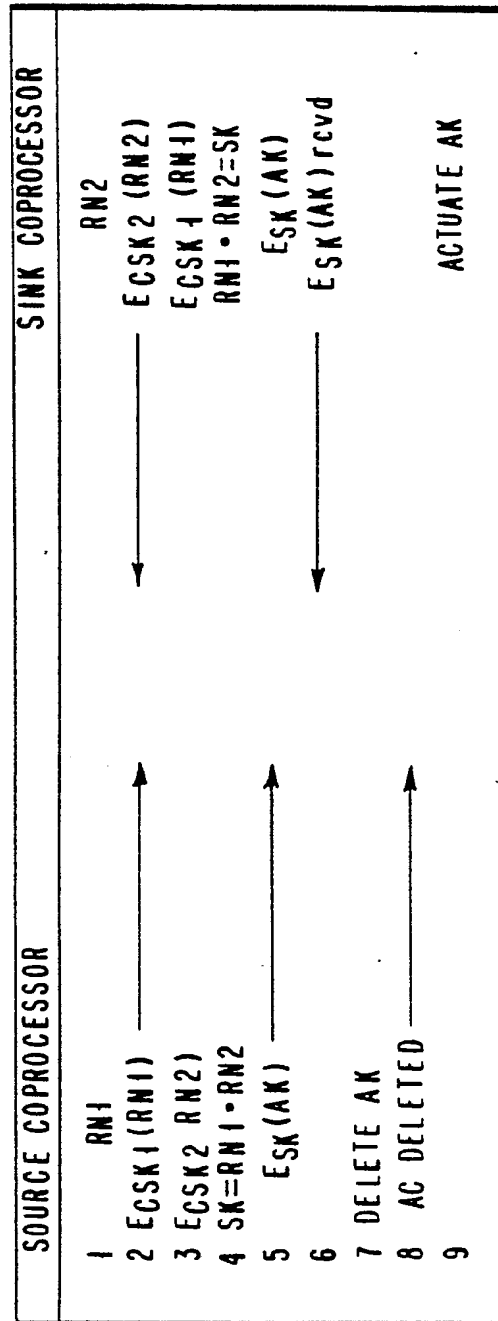


FIG. 21

(19)



Europäisches Patentamt
European Patent Office
Office européen des brevets



(11) Publication number:

0 464 306 A2

(12)

EUROPEAN PATENT APPLICATION(21) Application number: **91102317.4**(51) Int. Cl.5: **G06F 1/00**(22) Date of filing: **19.02.91**(30) Priority: **29.06.90 US 546334**(43) Date of publication of application:
08.01.92 Bulletin 92/02(84) Designated Contracting States:
AT BE CH DE DK ES FR GB IT LI NL SE(71) Applicant: **International Business Machines Corporation**
Old Orchard Road
Armonk, N.Y. 10504(US)(72) Inventor: **Hartrick, Thomas Vincent**

170 Sharpstead Lane
Gaithersburg, MD 20878(US)
Inventor: **Higgins, Patricia Eileen**
33 Oak Shade Road
Gaithersburg, MD 20878(US)
Inventor: **Sabia, Nicholas James**
2213 Drury Road
Silver Spring, MD 20906(US)

(74) Representative: **Jost, Ottokarl, Dipl.-Ing.**
IBM Deutschland GmbH Patentwesen und
Urheberrecht Schönaicher Strasse 220
W-7030 Böblingen(DE)

(54) **Structured document tags invoking specialized functions.**

(57) A system and method are disclosed for managing the display or the printing of a copyright notice or security label for a soft copy document, so as to provide appropriate security for the document as desired by its author. A special copyright notice can be displayed on the first page or predetermined pages of the document as it is displayed on a display screen. If a printer (44) is connected to the system and commanded to print the document, a cover page will be printed which includes the copyright notice, before the rest of the document is printed. If a "Do Not Copy" label is included in the soft copy of the structured document, any printer command, write to disk command, or telecommunication command will be aborted, thereby giving effect to the author's desired restriction not to copy the document.

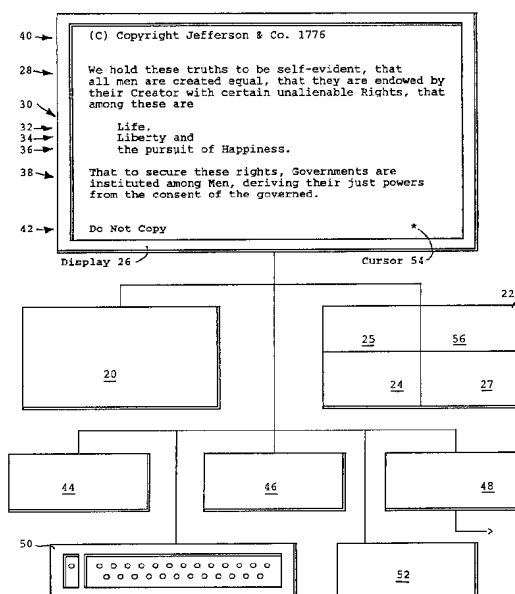


Fig. 1

EP 0 464 306 A2

Background of the Invention

1. Technical Field

The invention disclosed broadly relates to data processing and more particularly relates to the management of display and printing operations for a document by a data processor, so as to comply with proprietary and security restrictions of the document.

2. Background Art

Modern word processing and text editing programs employ structured document architecture to provide greater control and flexibility in the displayed and printed appearance of documents prepared with the programs. Structured document architecture is described, for example, in the copending European patent application EP-A-400 269 (IBM), entitled "A Method for Manipulating Elements Within a Structured Document Using Active Intent Interpretation," by C. J. Bennett, et al., incorporated herein by reference. A structured document can be prepared in accordance with the standardized general markup language, such as is described in the International Standard's Organization Standard 8879-1986. A data stream of text marked up in accordance with the standardized general markup language, will have its text divided into elements consisting of a begin tag and its content and terminated by an end tag, when necessary. Within a WYSIWYG (what you see is what you get) editor, text is displayed to the user as it will appear when it is printed, even though its structure is defined by the begin tags and end tags for each element of text. Formatting of the elements within a structured document is done when the document is displayed to the user. Those elements which fall into the category of commonly used elements include paragraphs, simple lists, ordered lists, bulleted lists, and list items.

Large documents marked up with structured document architecture tags, can be manipulated as an electronic book, by the method described in the copending European patent application EP-A-384 986 (IBM), entitled "A Method for Displaying On-Line Information," by E. Cassorla, et al., incorporated herein by reference. The European patent application EP-A-384 986 describes a method for creating on-line information from the same marked up source material used to create printed information such as a word processor or a markup language source used with a text formatter. A book data stream is provided, in an intermediate format for storing on-line information, specifically designed to be used by a book display program. The data stream captures and preserves structural informa-

tion about the books, by using the structured document tags. The method is suited to display on-line books in a useable manner on a variety of display devices. A book display program manipulates the book data stream and allows users to interact with the on-line information. The electronic book may be used like a hard copy book, except that it is displayed on a display screen. The method allows readers to treat on-line books as if they were hard copy books, and uses the book data stream as its input.

Electronic books are frequently communicated, stored, displayed and modified in their soft copy form, with hard copies only occasionally made. Authors of such electronic books or documents frequently desire to impose appropriate forms of security treatment for the electronic books so generated and they wish to have any rights of authorship in their works, respected. However, the prior art has not provided an adequate means to enforce the author's intentions for the treatment of his electronic books or documents. Although the author may place a copyright notice on his soft copy documents, there is no mechanism for increasing the prominence of that notice. Security labels such as "Company Confidential," "Do Not Copy," or "Do Not Distribute," which the author may place on the soft copy of the document, are not readily enforceable.

Terminology

The following terminology is used in this description, in referring to structured document architecture concepts.

SGML

Standardized General Markup Language. A markup language consisting of tags used to prepare structured documents. Refer to International Standards Organization standard 8879-1986 for definition and details.

Structured document

A document prepared in accordance with an SGML-compliant type definition.

Element

SGML-defined entity consisting of a begin tag and its alphanumeric string content, and including an end tag, when necessary.

Empty element

An element whose contents are null, containing

neither text nor other elements.

Current document position

The document position which determines the current page for display.

Commonly used elements

Those elements which fall into the category of commonly used elements include Paragraphs, Simple Lists, Ordered Lists, Bulleted Lists and List Items.

Tag name

The name given to a set of elements which all abide by the same rules of formatting. Examples of a tag name include **PARAGRAPH**, **SIMPLE LIST**, and **LIST ITEM**.

Formatted Text Stream

The formatted text stream is the sequence of alphanumeric characters which includes the structured document tags and associated text for the elements comprising the structured document.

Objects of the Invention

It is therefore an object of the invention to provide an improved method for managing the soft copy text of a structured document in a data processing system, so as to comply with proprietary and security restrictions of the document.

It is another object of the invention to provide an improved method for managing the display of pages from a structured document, so as to comply with proprietary and security restrictions of the document.

It is still a further object of the invention to provide an improved method for managing the printing of pages of a structured document, so as to comply with proprietary and security restrictions of the document.

It is yet another object of the invention to provide an improved method for managing the writing of a structured document into a bulk storage medium, so as to comply with proprietary and security restrictions of the document.

It is yet a further object of the invention to provide an improved method for managing the telecommunication of soft copies of a structured document, so as to comply with proprietary and security restrictions of the document.

It is still a further object of the invention to provide an improved method for managing the generation of acoustic enunciations corresponding to

indicia elements placed in a structured document.

Summary of the Invention

These and other objects, features and advantages of the invention are accomplished by the system and method for employing structured document tags to invoke specialized functions. The invention finds application in a data processing system which includes a processor for executing program instructions, a display device coupled to the processor for displaying a plurality of document elements in an ordered sequence in response to the program instructions, a memory in which is stored a structured document with its element tags, and a printer coupled to the processor for printing portions of the structured document stored in the memory. A method is disclosed for managing the display or printing of special indicia contained within the structured document. The special indicia are proprietary notices such as for copyright or security notices such as "Do Not Copy." The method will control the display or printing of the document so as to comply with the proprietary or security notices. The method includes the step of storing in the memory as a part of the structured document, a special indicium element containing a string representing the indicium, the element being identified by a special indicium tag. The method searches for the special indicium tag in the structured document, sets a flag in the memory when the special indicium tag is detected and loads the string representing the indicium into the memory. The method will display the special indicium on selected pages of the structured document when being displayed in WYSIWYG form by the display device. The special indicium can be printed on a cover page or selected pages of a hard copy of the document printed on a printer. Printing, copying and communications commands can be aborted in response to certain security indicia.

This feature can be employed to place a special copyright notice on the first page of the displayed document as it is displayed on the display device. The copyright notice element including the indicium string and its copyright tag preceding the string can be located anywhere in the structured document's formatted text stream. This is referred to as a global tag. If a printer is connected to the system and commanded to print the document, a cover page can be selectively printed, in accordance with the invention, which includes the copyright notice, before the rest of the structured document is printed by the printer.

The special indicium string can also be a security label such as a "Company Confidential" label, which is identified by a security tag preceding the string. In accordance with the invention, the secu-

urity label can selectively be displayed on all pages which are displayed in WYSIWYG form on the display device for the structured document. Alternately, if a printer is connected to the system and it is commanded to print the document, then in accordance with the invention, a cover page can selectively be generated upon which is printed the security label. The security label can also selectively be placed on each printed page of the structured document, by the printer.

The special indicium string can be a "Do Not Copy" label. A "Do Not Copy" label can be a special indicium string in the structured document identified by a "Do Not Copy" tag preceding the string, which can then be selectively displayed on all pages when the document is displayed on the display device. Still further, in accordance with the invention, if a printer connected to the system is commanded to print the document, the printing operation will be aborted in response to the presence of the "Do Not Copy" indicium. Still further and in accordance with the invention, if a disk drive storage device is connected to the system, a write to disk command for the document will be aborted in response to the "Do Not Copy" indicium. Still further, if a communications adapter is connected to the system, a transmission command for the document will have its function aborted in response to the "Do Not Copy" indicium.

An additional feature which is provided by the special indicium is the provision of a password. A password string can be embedded within the structured document text and identified by a special password tag preceding the string. When the initial search through the structured document identifies a password tag, before any further display or printing of the structured document is allowed, the method will present the user with a message that the user must enter a password. The password entered by the user, for example, must be identical to the embedded password string within the structured document text. Only if the user inputs the correct password, will further document display and printing functions be allowed, in accordance with the invention.

Another feature provided by the invention is the provision of local display or sound playing indicia elements. These are designated by local tags for the display of the special indicia only on the page of the document where the tag is located. If a local display indicium tag is provided, then when a particular page from the structured document bearing the local indicium tag is displayed on the display device, the associated special display indicium string will provide for the highlighting or other visual feature on that page. Alternately, if a "play sound" indicium tag is provided, then the string within the sound element will be transmitted to a

sound generating device connected in the system when the page of the structured document bearing the local sound indicium element, is displayed on the display device.

Brief Description of the Drawings

These and other objects, features and advantages of the invention will be more fully appreciated with reference to the accompanying figures.

- Fig. 1 is a system block diagram of the document manager system, in accordance with the invention.
- Fig. 2 is a first example of element tags and associated text.
- Fig. 3 illustrates the memory organization of element tags and associated text, for the example of Fig. 2.
- Fig. 4 is a diagram of the default parameter table.
- Fig. 5 is a diagram of the default parameter table after the initialization process of Fig. 7.
- Fig. 6 is a more detailed diagram of the memory image for a second example of the formatted text stream 25, showing in particular the element coordinates 156 associated with each particular element in the formatted text stream.
- Fig. 7 is a flow diagram of the initialization process.
- Fig. 8, consisting of Figs. 8A and 8B, is a flow diagram for displaying a document.
- Fig. 9, consisting of Figs. 9A and 9B, is a flow diagram for printing a document.
- Fig. 10 is a flow diagram for communicating a document over a communications link.
- Fig. 11 is a flow diagram for writing the document onto a magnetic disk storage medium.

Description of the Best Mode for Carrying Out the Invention

The document manager system shown in Fig. 1 includes a processor 20 connected to a display 26, to a memory 22, to a printer 44, a disk drive 46, a communications adapter 48, a keyboard 50 and an enunciator 52. The processor 20 executes program instructions 24 stored in the memory 22, which are represented by the flow diagrams of Figs. 7-11. The display device 26 coupled to the processor 20 displays in WYSIWYG form, a plurality of document elements such as paragraphs 28 and 38, list 30, which includes list items 32, 34 and

36 shown in the display device 26 of Fig. 1. Cursor 54 is also shown. The elements can include lists which are either ordered or unordered, and elements can also include graphics as well as text. Of special note is a copyright notice 40 and a "Do Not Copy" security label 42 displayed in WYSIWYG form for the page of the structured document shown on the display device 26 of Fig. 1. The document elements 28-42 are organized in a formatted text stream having an ordered sequence, as can be seen in Fig. 2, using structured document notation, where the ordered sequence is specified by a corresponding ordered sequence of the plurality of element tags. The paragraph 28 in Fig. 2 is shown in the structured document notation with the begin tag [p] and the end tag [/p]. Each element such as the paragraph 28 shown in Fig. 2, is a structured document element having a begin tag [p], the text of the paragraph in this example, and then an end tag [/p]. The begin tag and the end tag serve to identify the element type, in this case indicating a paragraph. The order of occurrence of the WYSIWYG display of paragraph 28 on the display device 26 is determined by the order of occurrence in the formatted text stream of the structured document element representing that paragraph 28 shown in Fig. 2, within the context of the order of occurrence of the other structured document elements, as for example, the list 30 and the paragraph 38.

In accordance with the invention, special strings such as a copyright notice or such as a security label, are embedded within special indicia elements having special structured document tags in the structured document. Specifically, the copyright notice element 40 is a string embedded between a begin tag [cpr] and an end tag [/cpr]. Similarly, the security label string "Do Not Copy" is embedded in the structured document text within a begin tag [sec2] and an end tag [/sec2]. When the processor 20 detects the presence of a special indicium tag such as a copyright begin tag or such as a security label begin tag, it makes special note of their presence within the memory 22, so that when specified display device 26, printer 44, disk drive 46, communications adapter 48 or enunciator 52 functions are requested, corresponding actions are taken in accordance with the type of special indicium. For example, if a "Do Not Copy" security element is identified in the document text, then the printer function will be inhibited if the user requests the printing of the structured document within which the "Do Not Copy" label is identified.

The order of occurrence of the structured document elements such as the paragraph 28, list 30 and paragraph 38, can be determined by their order of occurrence in the formatted text stream stored in the memory 22 as is shown in Fig. 3. Fig.

3 shows that the structured document text with its tags of Fig. 2, have been stored in the memory 22 in a linear sequential order, which is the formatted text stream 25. Paragraph element 28 includes tags 28a and 28b and text 28c. List element 30 includes tags 30a and 30b. List item element 32 includes tags 32a and 32b and text 32c. List item element 34 includes tags 34a and 34b and text 34c. List item element 36 includes tags 36a and 36b and text 36c. Paragraph element 38 includes tags 38a and 38b and text 38c.

The special copyright notice element is represented by the begin tag 40a and the end tag 40b which surrounds the copyright notice string 40c. Similarly, the special security label "Do Not Copy" element is represented by the begin tag 42a, and the end tag 42b, which surrounds the "Do Not Copy" string 42c. In accordance with the invention, when the processor 20 searches through the formatted text stream 25 stored in the memory 22 and detects the presence of the begin tag 40a or the end tag 40b for the copyright string 40c, the processor loads the copyright string 40c into a specified partition 60 of a parameter table 56 in the memory 22 and it sets a flag 62 to indicate the presence of a copyright string, as shown in Figs. 4 and 5. Correspondingly, if the processor 20 detects the presence of the begin tag 42a for the "Do Not Copy" string 42c, the processor will load the string 42c in the memory in a specified partition 60 and will set a flag 62 indicating that this type of security label is present in the structured document.

Still further in accordance with the invention, at the time of initial program loading for the program instructions 24 into the data processing system shown in Fig. 1, a default parameter table 56 is loaded into memory at a pre-specified partition. The default parameter table 56 shown in Fig. 4 will have a set of default values entered therein which are stored in the memory 22. Alternately, the user can enter a profile of values for the parameter table 56. The parameter table 56, as loaded at the initial program loading, will include the characters representing each special tag such as the copyright tag "cpr," a "Do Not Copy" tag "sec2," and the like, as is shown in Figs. 4 and 5. Also included in the parameter table 56 of Fig. 4 will be values indicating the response which the data processing system is to make when particular tagged strings are identified in the document text loaded into the memory 22. For example, if a copyright tag "cpr" is detected in a structured document, then the default parameter table 56 will indicate that if the document is to be displayed on the display 26, the first page displayed will include the copyright notice. If the document is to be printed by the printer 44, then a cover page will be generated with the copyright notice, prior to the printing of the structured

document.

Fig. 6 is a more detailed diagram of the memory image for a second example of the formatted text stream 25, showing in particular paragraph coordinates 156 associated with each particular paragraph, heading and other element in the formatted text stream 25. The formatted text stream 25 illustrated in Fig. 6 has structured document tags similar to those referenced above. The structured document tags for the chapter heading is the begin tag [h1] and the end tag [/h1]. Under the chapter heading, there are two elements, the first being a copyright notice element 140 represented by the special tag [cpr] followed by the special copyright notice string "(C) ABC Co 1990" and followed by the end tag [/cpr]. The second element under the chapter heading is a paragraph element denoted by a paragraph begin tag [p] and an end tag [/p]. The formatted text stream 25 is characterized by a hierarchical organization, in that the first topic heading depicted by its begin tag [h2] and end tag [/h2], is subsidiary to the chapter heading in the hierarchy. Use is made of this hierarchical structure for the formatted text stream 25, to establish the coordinate system 156. The coordinate system 156 is shown in Fig. 6 as it can be stored in memory 22, with four digits representing the hierarchical level of the particular heading or element entry to which the coordinate is associated. For example, the paragraph 142 has a coordinate of h1=1, h2=1, h3=0 and p=2. This means that the element 142 is part of the first h1 chapter heading, part of the first h2 topic heading, and is not part of any subsidiary topic heading to the first topic heading. The p=2 coordinate represents that the paragraph 142 is the second element under the first topic heading.

It is to be noted that there are two local tags in the formatted text stream 25 of Fig. 6, the first being at a first local element 150 which contains the begin tag [locC] followed by the "Sound String," which is followed by the end tag [/locC]. The coordinates for the element 150 are 1101. The first local element 150 will be given effect by playing the desired sound on the enunciator 52, as specified by the sound string, when the page containing the element is to be displayed on the display 26.

Fig. 6 shows a second local element 160 which includes the begin tag [locA] followed by the "Display String," which is followed by the end tag [/locA]. Second local element 160 has the coordinates 1211. The second local element 160 will be given effect on display 26 when the page containing the second local element 160 is displayed by the display 26.

The formatted text stream 25 of Fig. 6 further includes an element 170 which is a security ele-

ment containing the begin tag [sec2] followed by the string "Do Not Copy," which is followed by the end tag [/sec2]. The copyright notice element 140 and the "Do Not Copy" notice element 170 are global elements which will be given effect, without regard for the location at which the element occurs in the formatted text stream 25.

Fig. 7 is a flow diagram of the initialization of the system of Fig. 1, loading the parameter table 56 into the memory 22 and setting the values of the parameters therein, in accordance with the occurrence of particular special elements which may occur in the formatted text stream 25. The flow diagram of Fig. 7 starts with step 90 which loads the parameter table 56 of Fig. 4, containing the default names of the tags and the default functions to be performed by the display device 26, printer 44, disk drive 46, communications adapter 48, and enunciator 52 in response to the occurrence of any of the special tags occurring in the formatted text stream 25. It is the objective of the flow diagram of Fig. 7 to scan through the formatted text stream 25 and identify special tags for special elements and to load the corresponding strings into the default parameter table 56 and turn on the corresponding flags in the default parameter table 56 so that there results a table 56 such as is shown in Fig. 5. Step 90 loads the parameter table 56 of Fig. 4 into the memory 22 and step 100 inputs the formatted text stream 25 of the structured document and stores it in memory 22. Step 100 then flows into step 101 where a print session flag is set and a copy session flag is set. As will be described later, the first time that the user wishes to print any portion of the formatted text stream which was input in step 100, special notices can be displayed as set forth for steps 305 and 307 in Fig. 9, after which step 309 will turn off the print session flag so that subsequent commands to print portions of the same document will not result in the repeated display of warning messages and notices. The copy session flag will have a similar effect the first time that the user commands that the formatted text stream be communicated in Fig. 10 or written to a disk as provided in Fig. 11. In Fig. 7, step 101 then flows to step 102. Then step 102 searches for any special indicium tag as specified by the default expressions for the tags in column 64 of the default parameter table 56 of Fig. 4. In step 104, if any special tag is found, then in step 106 the corresponding flag in column 62 of table 56 is turned on. Then in step 107, the string enveloped by the special begin tag and its corresponding end tag is loaded into column 60 of table 56. For example, in the formatted text stream 25 of Fig. 6, the search step 102 will identify element 140 which is a copyright notice string, by the [cpr] special tag. The corresponding flag in column 62 will be turned on

and the string "(C) ABC Co 1990" will be stored in the column 60 of the default parameter table 56, as is shown in Fig. 5.

Then, the flow diagram of Fig. 7 will have step 108 determine whether the tag is a global tag. The tags "locA," "locB," and "locC" are all local tags, the rest of the tags represented in column 64 of table 56 being global tags. Since the [cpr] tag is a global tag, a determination is made in step 110 as to whether the tag is a password tag, that is whether it is [pswd]. If it is a password tag, then the process flows to step 112 which asks the user to input the password, the true password being stored in a string within the formatted text stream 25, associated with the password tag. If the user inputs the correct password, as determined in step 114, then the process flows to step 118. However, if the user fails to input the correct password, the process flows to step 116 which aborts any further operations and the process returns to the main program. A notice can be displayed to the user that the password was not correct. Alternately, if the tag is not a password tag as determined in step 110, then a process flows to step 118.

If step 108 determines that the tag is a local tag, as determined by column 64 of the default parameter table 56, then the coordinate for the local tag element is stored in column 66 of the table 56 in step 120. Thereafter, the process flows to step 118.

In step 118, it is determined if there is any more text to be scanned in the formatted text stream and if there is, then the process flows back to step 102 to search for any additional special indicium tags. Alternately, if there is no more text to be scanned, then the flow returns to the main program. At the end of the operation set forth in the flow diagram of Fig. 7, the default parameter table 56 will be populated as is shown in Fig. 5, with those special elements which have been detected in the formatted text stream 25, having their corresponding text strings loaded into column 60 of table 56, the corresponding flag turned on in column 62 and, for local tags, the corresponding local coordinates loaded in column 66. Fig. 5 shows that there are two global special elements, element 140 which is a copyright notice element and element 170 which is a "Do Not Copy" notice element, and that there are also two local special elements, a sound element 150 and a display string element 160.

Fig. 8 is a flow diagram of the sequence of operational steps for displaying the formatted text stream 25 on the display 26. In step 200, the user requests a WYSIWYG display of the formatted text stream 25. In step 202, a page of the formatted text stream is loaded into a display buffer. In step 204, the default parameter table 56 is interrogated to

determine if there is a global copyright flag turned on in column 62. If yes, then step 206 determines from table 56 whether the copyright notice is to be displayed on the first displayed page on the display 26. If yes, then step 208 displays the copyright notice on the first displayed page. The process then flows to step 210 which determines whether table 56 specifies that the copyright notice is to be displayed on all pages displayed on the display 26. If yes, then each page of the formatted text stream 25 which is displayed would include a copyright notice at the appropriate location on the display screen of display 26. However, in the example of Fig. 5, there is no requirement for the display of the copyright notice on each page. The process then flows to step 214 which determines whether a security label with a [sec1] tag has its flag turned on in column 62 of the default parameter table 56. If it does, then the process flows to steps 216 and 218 which are similar to steps 206 and 210, respectively. The process then flows to step 220 which determines whether there is a "Do Not Copy" label corresponding to a [sec2] tag with its flag on in column 62 of the default parameter table 56. If there is, then the process flows to steps 222 and 224 which are similar to steps 206 and 210. In this example, there is a "Do Not Copy" label since the flag is on in column 62. The default parameter table 56 shows that the "Do Not Copy" label is to be applied to every page displayed on the display 26. Therefore, step 224 determines that the "Do Not Copy" label will be displayed on every page.

The process then flows to step 226 which determines whether there is a restriction element present and if so, then the process flows to steps 228 and 230, which are similar to steps 206 and 208. In this example, there is no restriction element corresponding to the tag [rest]. Restriction elements can be for example, a limited rights notice which the author wishes to place in his documentation. Typically the limited rights notice would be placed on the first page to be displayed to the reader, along with copyright notice and any security notice such as a confidential information label.

The process then flows to step 232 which determines if there are any local tags present, by determining if there are any corresponding flag bits turned on in column 62 of table 56. In this example, there are two bits turned on in column 62. Therefore, the process of Fig. 8 flows to step 234 which determines if the local coordinates in column 66 of table 56 are on the current page being displayed on the display 26. If they are, then the process flows to step 236 to determine if the local special element is a sound-type element having a "[locC]" tag. If it is, then the process flows to step 238 where the sound string is transferred from column

60 in table 56 to the enunciator 52 associated with the processor 20 to play the sound specified by the sound string. This is the case for the example of Fig. 5, where if the page being displayed on the display 26 includes the element coordinates 1101, then the sound string is played at this time. The process then flows to step 240 which determines if there is a local special element of the display type, having a tag "[locA]," for the page currently displayed on the display 26. If yes, then step 242 either displays the corresponding string stored in column 60 of the default parameter table 56 or alternately, executes a display-type command, such as a reverse video highlight for the page being displayed. This is the case for the example of Fig. 5 where, if the element coordinate 1211 is present in the page being displayed on display 26, then a reverse video highlighting is provided for the page being displayed.

The process of Fig. 8 then flows to step 244 to determine whether there is another page of text in the formatted text string 25 to be displayed. If there is, then the process flows to step 202 to load the next page into the display buffer and the flow diagram of Fig. 8 continues. If not, then the process returns to the main program.

Fig. 9 is a flow diagram of the sequence of operational steps for printing the formatted text stream 25 with the printer 44. The process begins with step 300 wherein the user requests the printing of the formatted text stream. Then step 302 loads a page into a buffer for printing. Step 304 interrogates the default parameter table 56 to determine if there is a special copyright element with a flag bit on in column 62. The process then flows to step 305 which determines if the print session flag is on. If it is on, then the process flows to step 307 where a notice is displayed on the display 26 with the copyright string. A prompt symbol is presented to the user requesting whether the user wishes to continue. The user must affirmatively indicate his desire to continue by depressing a key on the keyboard 50, for example. Step 309 turns off the print session flag. In this manner the notice of 307 is displayed only the first time a command is made in step 300. Then in step 311, it is determined whether the user has indicated his desire to continue. If yes, then the process flows to step 306. If step 311 determines that the user indicates he does not wish to continue, then the process returns to the main program. This provision of a user option to continue, could also be employed for the SEC1 flag following step 314 and the restricted materials "rest" flag following step 326. Step 306 determines whether a cover page is to be printed prior to the printing of any other page of the document, displaying the copyright notice from the copyright string stored in column 60 of the default

parameter table 56. In the case of the example shown in Fig. 5, a cover page is required and therefore step 308 prints a cover page containing the copyright notice "(C) ABC Co 1990." Then step 310 determines whether the copyright notice is to be printed on all pages. If it is, then step 312 will print the copyright notice string on all pages. The process then flows to step 314 where it is determined whether a security label is to be printed, by determining the presence of a corresponding flag bit in column 62 of table 56. If it is, then step 316 determines whether the security label is to be printed on a cover page preceding all other pages of the document. Then step 318 determines whether the security label is to be printed on every page of the document. In the case of the example in Fig. 5, there is no security label corresponding to the tag "[sec1]."

Step 320 then determines whether there is a "Do Not Copy" special element by determining whether there is a corresponding flag bit on in column 62 of table 56. In the case of the example of Fig. 5, there is a "Do Not Copy" label and therefore the process of Fig. 9 flows to step 322 which aborts the print command. At this time, a notice can be displayed on the display device 26 indicating that this is a "Do Not Copy" document, and printing has been terminated. The process will then return to the main program. Alternately, if step 320 determines that there is no "Do Not Copy" element, then the process flows to step 326 which determines whether there is a restriction element present by determining whether there is a corresponding flag bit turned on in column 62 of table 56. If there is, then the process flows to steps 328 and 330 which are similar to steps 306 and 310 above. The process then flows to step 344 to determine if there is another page to be printed. If there is, then the process flows back to step 302 to load the next page into the buffer for printing. If there is no next page, then the process returns to the main program.

Fig. 10 is a flow diagram of a sequence of operational steps to carry out the communication of the formatted text stream over a communications link using the communications adapter 48. The process begins with step 400 wherein the user requests the communication of the formatted text stream 25. Step 402 then determines whether there is a "Do Not Copy" security tag "[sec2]" or alternately a "Do Not Send" element with a tag "[sec3]" as would be determined by corresponding flag bits being on in column 62 of table 56. If there is, then the process flows to step 404 where the communications operation is aborted, and then it flows to step 406 where a notice is displayed on the display screen 26 that this is either a "Do Not Copy" or a "Do Not Send" document. The process

then returns to the main program. Alternately, if step 402 determines that there is no "Do Not Copy" or "Do Not Send" label in the parameter table 56, then the process flows to step 403' where it is determined whether the copyright flag is present. If the copyright flag is present, the process flows to step 405 to determine if the copy session flag is on. If it is on, then the process flows to step 407' where the copyright string is displayed on the display 26 and a prompt is also displayed to the user requesting whether the user wishes to continue. If the user wishes to continue, the user must so indicate by pressing a key on the keyboard 50. Step 409 turns off the copy session flag. In this manner the notice to step 407 is displayed only the first time a command is made in step 400. Step 411' determines whether the user has indicated he wishes to continue. If the user wishes to continue, then the process flows to step 408. If the user indicates he does not wish to continue, then the process returns to the main program. Step 408 carries out the operation of sending the formatted text stream 25 over a communications link using the communications adapter 48. The process then returns to the main program.

Fig. 11 illustrates a flow diagram of a sequence of operational steps to carry out the writing of the formatted text stream 25 onto a magnetic storage disk using the disk drive 46. The process begins with step 420 wherein the user requests the write to disk operation. Then in step 422 it is determined whether there is a "Do Not Copy" element in table 56, by determining if the corresponding flag bit in column 62 is turned on. In the case of the example in Fig. 5, there is a "Do Not Copy" element present, and therefore the process flows to step 424 where the write to disk operation is aborted and then it flows to step 426 wherein a notice is displayed on the display 26 that this is a "Do Not Copy" document. This is followed by a return to the main program. Alternately, if step 422 determines that there is no "Do Not Copy" element in the formatted text stream 25, then the process flows to step 304" where it is determined whether the copyright flag is present. If the copyright flag is present, then the process flows to step 425 to determine if the copy session flag 425 is on. If it is on, the process flows to step 427 where the copyright string is displayed on the display 26 and the prompt is also displayed to the user requesting the user as to whether he wishes to continue. If the user wishes to continue, then the user must so indicate by pressing a key on the keyboard 50. Step 429 turns off the copy session flag. In step 431, it is determined whether the user has indicated he wishes to continue. If yes, then the process flows to step 428. Alternately, if the user indicates he does not wish to continue, then the

process returns to the main program. In step 428 the write operation is carried out writing the formatted text stream 25 onto a magnetic disk using the disk drive 46. The process then returns to the main program.

It is seen that the invention as disclosed herein provides an improved method for managing soft copy text of a structured document. The invention provides an improved method for displaying pages from a structured document in accordance with security restrictions imposed by its author. The invention further provides an improved method for managing the printing of the pages of a soft copy document, while maintaining the security restrictions imposed by its author. The invention further provides a flexible means for managing the copying or telecommunication of a soft copy of a structured document, in accordance with the security restrictions imposed by its author. Still further, the invention provides a flexible means for customizing the visual highlighting and for providing acoustical enunciations for localized portions of a soft copy document being displayed on a display screen.

A number of alternatives can be selected for the functioning of the tags set forth herein. For example, the local tag "locA" which is a local display tag shown in the default parameter table of Fig. 4, can have the local effect within the text where it is embedded, of prohibiting the display of the text if the user has not presented an appropriate password "pswd." This would enable an author to enforce a confidential restricted treatment for those portions of his document where the "locA" tag is embedded.

Although a specific embodiment of the invention has been disclosed, it will be understood by those having skill in the art that changes can be made in that specific embodiment without departing from the spirit and the scope of the invention.

One embodiment of this invention is a computer method for managing the display of pages of a structured document on a display device in a system, so as to comply with proprietary restrictions of the document, comprising the steps of: inputting into a computer system, a formatted text stream of a structured document which includes a proprietary notice element having a special tag and a proprietary notice character string; searching said formatted text stream to identify said special tag and storing said proprietary notice string in a memory in said system; receiving a command to display said document on a display device in said system; accessing said proprietary notice string and displaying it on said display device juxtaposed with a first occurring page to be displayed of said document.

A second embodiment of this invention is a

computer method for managing the display of pages of a structured document on a display device in a system, so as to comply with restriction notices in the document, comprising the steps of: inputting a control table into a computer system, specifying a first procedure for displaying a structured document in response to detecting a first type restriction notice in the document and specifying a second procedure for displaying a structured document in response to detecting a second type restriction notice in the document; inputting into said computer system, a formatted text stream of a structured document which includes a restriction notice element having a special tag and a restriction notice character string; searching said formatted text stream to identify said special tag and storing said restriction notice string in a memory in said system; receiving a command to display said inputted document on a display device in said system; determining whether said restriction notice in said inputted document is said first type or said second type; accessing said table to determine whether said first or said second procedure is a determined procedure to be used to display said inputted document, in response to said determining step; accessing said restriction notice string and displaying it on said display device associated with a display of said document, in accordance with said determined procedure.

A third embodiment of this invention is a computer method for managing the printing of pages of a structured document on a printer device in a system, so as to comply with proprietary restrictions of the document, comprising the steps of: inputting into a computer system, a formatted text stream of a structured document which includes a proprietary notice element having a special tag and a proprietary notice character string; searching said formatted text stream to identify said special tag and storing said proprietary notice string in a memory in said system; receiving a command to print said document on a printer device in said system; accessing said proprietary notice string and printing it on a cover page with said printer device prior to printing a first occurring page to be printed of said document.

A fourth embodiment of this invention is a computer method for managing the printing of pages of a structured document on a printer device in a system, so as to comply with copy restrictions of the document, comprising the steps of: inputting into a computer system, a formatted text stream of a structured document which includes a copy restriction notice element having a special tag and a restriction notice character string;

searching said formatted text stream to identify said special tag and storing said restriction notice string in a memory in said system; receiving a command to print said document on a printer device in said system; accessing said restriction notice string and displaying it on a display device in said system in response to said command to print; aborting said command to print said document in response to identifying said special tag.

A fifth embodiment of this invention is a computer method for managing the printing of pages of a structured document on a printer device in a system, so as to comply with restriction notices in the document, comprising the steps of: inputting a control table into a computer system, specifying a first procedure for printing a structured document in response to detecting a first type restriction notice in the document and specifying a second procedure for printing a structured document in response to detecting a second type restriction notice in the document; inputting into said computer system, a formatted text stream of a structured document which includes a restriction notice element having a special tag and a restriction notice character string; searching said formatted text stream to identify said special tag and storing said restriction notice string in a memory in said system; receiving a command to print said inputted document on a printer device in said system; determining whether said restriction notice in said inputted document is said first type or said second type; accessing said table to determine whether said first or said second procedure is a determined procedure to be used to print said inputted document, in response to said determining step; accessing said restriction notice string and printing it on said printer device associated with a printing of said document, in accordance with said determined procedure.

A sixth embodiment of this invention is a computer method for managing the display of special indicia contained within a structured document, on a display device in a system, comprising the steps of: storing in a memory in said system as a part of a structured document, a special indicium identified by a special indicium tag; searching for said special indicium tag in said structured document; setting a flag in said memory when said special indicium tag is detected; displaying said special indicium on a predetermined page of said structured document when being displayed by said display device.

This sixth embodiment further comprises said predetermined page being the first page of said structured document displayed by said display device;
 said special indicium being displayed on each page of said structured document when being displayed by said display device;
 said special indicium being displayed on the same page where said special indicium tag is located in said structured document.

The said special indicium is a visual highlighting of the page being displayed, an acoustical enunciation played by an acoustical enunciator associated with said display device, a copyright notice or a security label.

A seventh embodiment of the invention is a method for managing the printing of special indicia contained within a structured document, on a printing device, comprising the steps of:

storing in a memory as a part of a structured document, a special indicium identified by a special indicium tag;
 searching for said special indicium tag in said structured document in said memory;
 setting a flag in said memory when said special indicium tag is detected;
 printing said special indicium on a predetermined page of said structured document when being printed by said printing device.

In this embodiment the predetermined page may be a cover page which precedes the printing of said structured document by said printing device.

In this embodiment the special indicium can be printed on each page of said structured document when being printed by said printing device and may be either a copyright notice or a security label.

An eighth embodiment of the invention is a method for managing the printing of a structured document having a "Do Not Copy" restriction, comprising the steps of:

storing in the memory as a part of a structured document, a special indicium identified by a special indicium tag indicating that the document is not to be copied;
 searching for said special indicium tag in said structured document in said memory;
 prohibiting said structured document from being printed by a printer coupled to said memory, in response to detecting said special indicium in said structured document.

A ninth embodiment of this invention is a method for managing the telecommunication of a structured document having a "Do Not Copy" restriction, comprising the steps of:

storing in the memory as a part of a structured document, a special indicium identified by a spe-

cial indicium tag indicating that the document is not to be copied;
 searching for said special indicium tag in said structured document in said memory;
 prohibiting the transmission of said structured document, in response to detecting said special indicium in said structured document.

A tenth embodiment of the invention is a method for managing the copying of a structured document onto a magnetic disk storage medium, comprising the steps of:

storing in the memory as a part of a structured document, a special indicium identified by a special indicium tag indicating that the document is not to be copied;
 searching for said special indicium tag in said structured document in said memory;
 prohibiting the copying of said structured document onto a magnetic disk storage medium.

An eleventh embodiment of the invention is a method for managing the password security access to a structured document, comprising the steps of:
 storing in a memory as a part of a structured document, a special indicium identified by a special indicium tag, indicating a valid password;
 requesting a user to input a test password before allowing the user access to said structured document;
 comparing said test password to said valid password and prohibiting the user from access to said structured document if they do not compare.

A twelfth embodiment of the invention is a method for managing the playing of special sounds corresponding to special indicia contained within a structured document, on an enunciator device, comprising the steps of:

storing in a memory as a part of a structured document, a special indicium identified by a special indicium tag;
 searching for said special indicium tag in said structured document in said memory;
 recording the location of said special indicium tag in said structured document, corresponding to a page thereof;
 enunciating a sound specified by said special indicium when said page of said structured document which includes said special indicium tag, is displayed by a display device.

A thirteenth embodiment of the invention is a system for managing the display of special indicia contained within a structured document, on a display device, comprising:

a memory in said system having stored therein a structured document which includes a special indicium identified by a special indicium tag;
 a processor coupled to said memory, for searching said structured document within said memory to locate and identify said special indicium tag there-

in;
 said processor setting a flag in said memory when said special indicium tag is detected;
 a display device coupled to said processor for displaying said special indicium on a predetermined page of said structured document when said structured document is being displayed by said display device.

A fourteenth embodiment of the invention is a system for managing the printing of special indicia contained within a structured document, on a printer, comprising:

a memory having stored therein a structured document which includes a special indicium identified by a special indicium tag;

a processor coupled to said memory for searching for said special indicium tag in said structured document in said memory;

said processor setting a flag in said memory when said special indicium tag is detected;

a printer coupled to said processor, for printing said special indicium on a predetermined page of said structured document when said structured document is being printed by said printer.

A fifteenth embodiment of the invention is a computer apparatus for managing the display of pages of a structured document on a display device in a system, so as to comply with proprietary restrictions of the document, comprising:

a memory in said system for receiving and storing a formatted text stream of a structured document which includes a proprietary notice element having a special tag and a proprietary notice character string;

a processor in said system coupled to said memory for searching said formatted text stream to identify said special tag and storing said proprietary notice string in said memory in said system;

said system receiving a command to display said document on a display device coupled to said processor in said system;

said processor accessing said proprietary notice string and displaying it on said display device juxtaposed with a first occurring page to be displayed of said document.

A sixteenth embodiment of the invention is a computer apparatus for managing the printing of pages of a structured document on a printer device in a system, so as to comply with proprietary restrictions of the document, comprising:

a memory in said system for receiving and storing formatted text stream of a structured document which includes a proprietary notice element having a special tag and a proprietary notice character string;

a processor in said system coupled to said memory for searching said formatted text stream to identify said special tag and storing said propri-

etary notice string in said memory in said system;
 said system receiving a command to print said document on a printer device coupled to said processor in said system;

5 said processor accessing said proprietary notice string and printing it on a cover page with said printer device prior to printing a first occurring page to be printed of said document.

A seventeenth embodiment of the invention is a computer apparatus for managing the printing of pages of a structured document on a printer device in a system, so as to comply with copy restrictions of the document, comprising:

15 a memory in said system for receiving and storing a formatted text stream of a structured document which includes a copy restriction notice element having a special tag and a restriction notice character string;

a processor in said system coupled to said memory for searching said formatted text stream to identify said special tag and storing said restriction notice string in said memory in said system;

20 said system receiving a command to print said document on a printer device coupled to said processor in said system;

said processor accessing said restriction notice string and displaying it on a display device in said system coupled to said processor in response to said command to print;

25 said processor aborting said command to print said document in response to identifying said special tag.

An eighteenth embodiment of the invention is a computer method for managing the printing of pages of a structured document on a printer device in a system, so as to comply with restrictions of the document, comprising the steps of:

inputting into a computer system, a formatted text stream of a structured document which includes a restriction notice element having a special tag and a restriction notice character string;

30 searching said formatted text stream to identify said special tag and storing said restriction notice string in a memory in said system;

40 receiving a command to print said document on a printer device in said system;

displaying on a display device said restriction string and presenting a prompt requesting whether the user wishes to continue;

50 receiving a signal from the user indicating that the user wishes to continue, and in response thereto, printing said restriction notice string with said printer device while printing said document;

alternately receiving an indication from the user that the user does not wish to continue, and in response thereto, aborting said command to print.

This embodiment further comprises the steps of:

receiving a second command to print said document on said printer device in said system; immediately accessing said restrictive notice string and printing it on a cover page with said printer device prior to printing a first occurring page to be printed of said document.

Claims

1. System for reproducing the contents of a structured document so as to comply with proprietary and security restrictions of the document comprising
 - a processor (20);
 - means for reproducing the contents of the said structured document connected to the said processor (20) and
 - a memory (22) which is connected to the said processor (20) and to the said means for reproducing the contents of the said structured document and into which is placed the said structured document as a formatted text stream including indicia to indicate said proprietary and security restrictions and indicum tags to indicate when such proprietary and security restrictions should be used.
2. System for reproducing the contents of a structured document according to claim 1 in which said proprietary restrictions include copyright display notices.
3. System for reproducing the contents of a structured document according to claim 1 in which said security restrictions include
 - a "company confidential" restriction.
4. System for reproducing the contents of a structured document according to claim 1 in which said security restrictions include
 - a "do not copy" restriction to prevent the copying of the document.
5. System for reproducing the contents of a structured document according to claim 1 in which said security restrictions include
 - a "do not send" restriction to prevent transmission of the document.
6. System for reproducing the contents of a structured document according to claim 1 fur-

ther comprising

an enunciator (52) to produce a sound on detection of the appropriate indicum.

7. System for reproducing the contents of a structure document according to claim 1 in which said means for reproducing the contents of the said structured document comprise
 - a display (26) for displaying the document.
8. System for reproducing the contents of a structure document according to claim 1 in which said means for reproducing the contents of the said structured document comprise
 - a disc drive (46) for storing the document on disc.
9. System for reproducing the contents of a structure document according to claim 1 in which said means for reproducing the contents of the said structured document comprise
 - a communications adapter (48) for transmitting the document.
10. System for reproducing the contents of a structure document according to claim 1 in which said means for reproducing the contents of the said structured document comprise
 - a printer (44) for printing the document.
11. Method for reproducing the contents of a structured document stored in a system so as to comply with the proprietary and security restrictions of the document comprising
 - loading a parameter table (56) into a memory (22), the said parameter table (56) specifying the procedures for complying with the proprietary and security restrictions of the document;
 - inputting into the said system a formatted text stream (25) of a structured document including indicia to indicate said proprietary and security restrictions and indicum tags to indicate when such proprietary and security restrictions should be used;
 - searching said formatted text stream (25) to identify said indicia and said indicum tags;
 - using the said identified indicia and indicum tags in conjunction with the said parameter table (56) to produce a modified parameter

table indicating which procedures are to be used to reproduce the contents of the said structured document;

reproducing the contents of the said structured document.

- 12.** Method for reproducing the contents of a structured document according to claim 11 in which said indicum tags include

indicum tags to indicate that the said proprietary or security restrictions should be implemented on every page of the said structured document.

- 13.** Method for reproducing the contents of a structured document according to claim 11 in which said indicum tags include

tags to indicate that the said proprietary or security restrictions should be implemented on selected pages of the said structured document.

- 14.** Method for reproducing the contents of a structured document according to claim 11 in which said indicum tags include

tags to indicate that the said proprietary or security restrictions should be implemented only on the cover page of the said structured document.

- 15.** Method for reproducing the contents of a structured document according to one of claims 11-14 in which said indicia include

a notice to indicate copyright restrictions of the said structured document.

- 16.** Method for reproducing the contents of a structured document according to one of claims 11-14 in which said indicia include

instructions to prevent the printing of one or more pages of the said structured document.

- 17.** Method for reproducing the contents of a structured document according to one of claims 11-14 in which said indicia include

instructions to prevent the copying of one or more pages of the said structured document.

- 18.** Method for reproducing the contents of a structured document according to one of claims 11-14 in which said indicia include

instructions to prevent the transmission of one or more pages of the said structured document.

- 19.** Method for reproducing the contents of a structured document according to one of claims 11-14 in which said indicia include

instructions to print a notice on chosen pages of the said structured document.

- 20.** Method for reproducing the contents of a structured document according to one of claims 11-19 further comprising

indicia to request the input of a password before parts of the said structured document can be reproduced.

- 21.** Method for reproducing the contents of a structured document according to one of claims 11-20 in which said indicia further include

instructions to produce a sound during reproduction of parts of said structured document.

- 22.** Method for reproducing the contents of a structured document according to one of claims 11-20 in which said indicia further include

instructions to display the said structured document in reverse video.

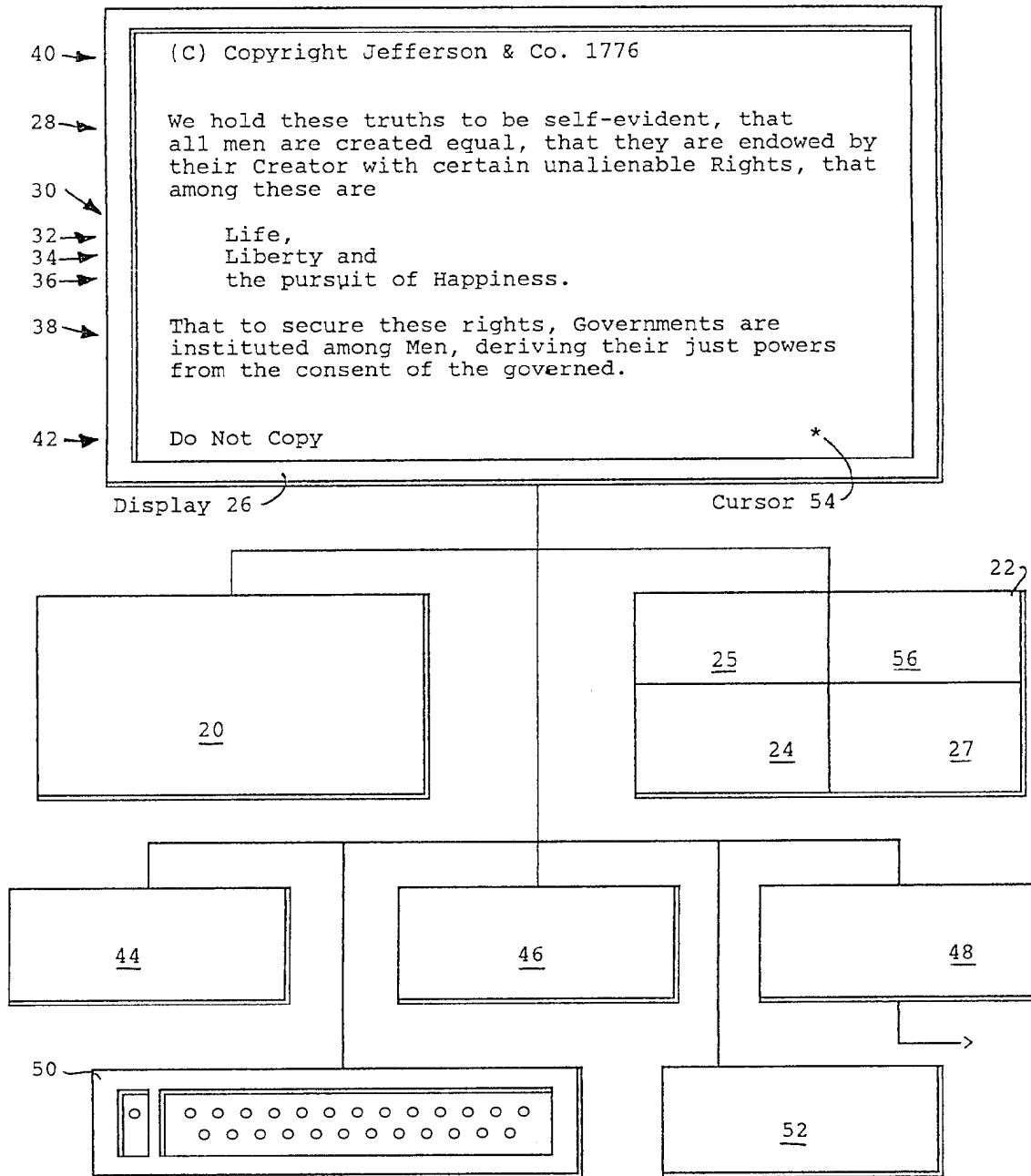


Fig. 1

[cpr](C) Copyright Jefferson & Co. 1776[/cpr] ← copyright 40
 [p]We hold these truths to be self-evident, that
 all men are created equal, that they are endowed by
 their Creator with certain unalienable Rights, that
 among these are[/p] ← paragraph 28
 [list] ← list 30
 [li]Life, [/li] ← 32
 [li]Liberty and[/li] ← 34
 [li]the pursuit of Happiness. [/li] ← 36
[/list]
[p]That to secure these rights, Governments are
instituted among Men, deriving their just powers
from the consent of the governed. [/p] ← paragraph 38
[sec2]Do Not Copy[/sec2] ← security 42
 25

Fig. 2

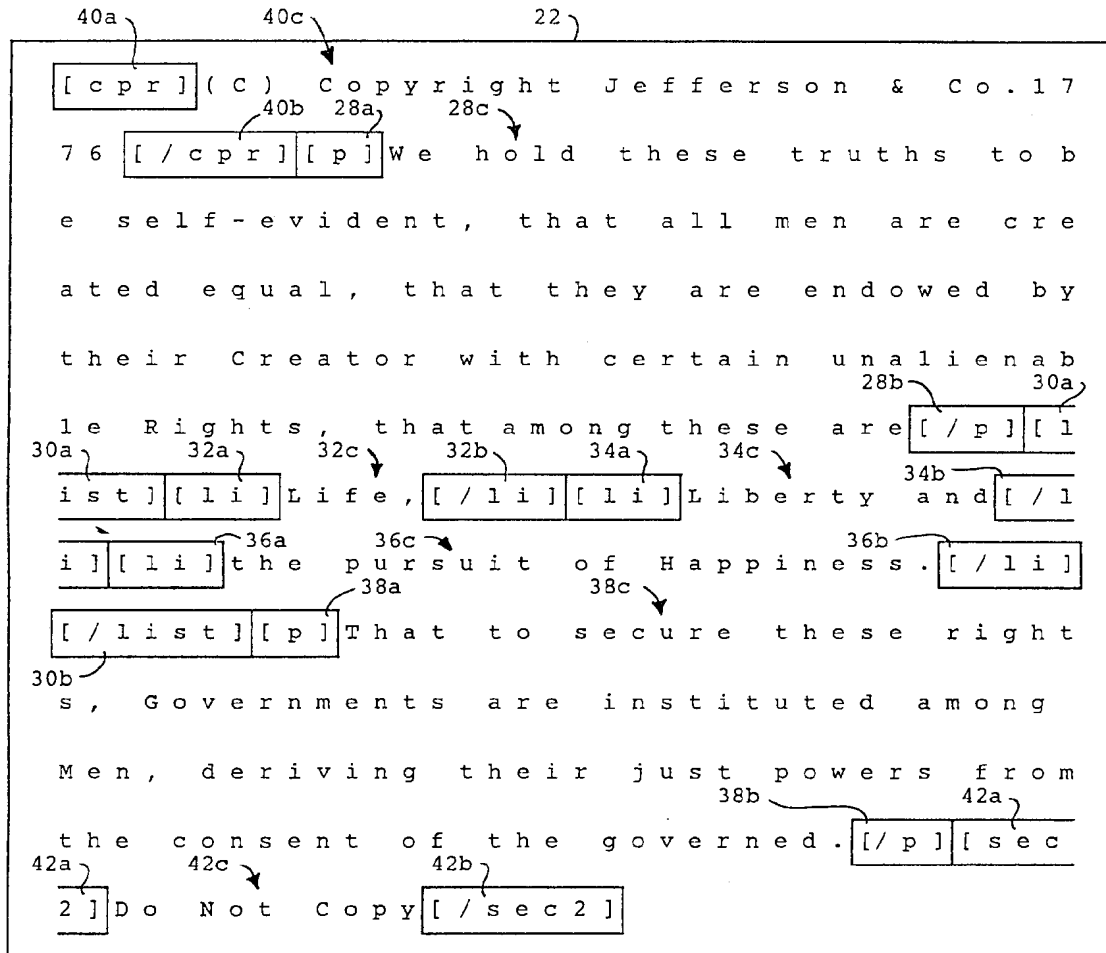


Fig. 3

56

Tag	Strings Loaded from Tagged Text	On	Display			Printer			Disk Drive abort	Communi- cate abort	Sound play
			1st page	all pages	local elmnt coord	cover page	all pages	abort			
cpr	Copyright		x			x					
sec1	Security Label			x		x	x				
sec2	Do Not Copy			x				x	x	x	
sec3	Do Not Send									x	
rest	Restriction		x			x					
pswd	Password										
	Local Page:										
locA	A (display)										
locB	B (voice)										x
locC	C (sound)										x

↑ 64 ↑ 60 ↑ 62 ↑ 66

Fig. 4

56 ↘

Tag	Strings Loaded from Tagged Text	Fl ag on	Display			Printer			Disk Drive abort	Commu- nicate abort	Sound play
			1st page	all pages	local elmnt coord	cover page	all pages	abort			
cpr	(C) ABC Co 1990	x	x			x					
sec1	Security Label			x		x	x				
sec2	DO NOT COPY	x		x				x	x	x	
sec3	Do Not Send									x	
rest	Restriction		x			x					
pswd	Password										
	Local Element:										
locA	reverse video	x			1211						
locB	B (voice)										x
locC	10101110	x			1101						x

↑ 64 ↑ 60 ↑ 62 ↑ 66

Fig. 5

25 ↗

156 ↗

		h1	h2	h3	p	/w
	[h1] Chapter Heading [/h1]	1	0	0	0	
140 →	[cpr] (C) ABC Co 1990 [/cpr]	1	0	0	1	
	[p] Paragraph of text [/p]	1	0	0	2	
	[h2] First topic heading [/h2]	1	1	0	0	
150 →	[locC] Sound String [/locC]	1	1	0	1	
142 →	[p] Paragraph of text [/p]	1	1	0	2	
	[h2] Second topic heading [/h2]	1	2	0	0	
	[p] Paragraph of text [/p]	1	2	0	1	
	[h3] First subtopic heading [/h3]	1	2	1	0	
160 →	[locA] Display String [/locA]	1	2	1	1	
	[p] Paragraph of text [/p]	1	2	1	2	
	[h2] Third topic heading [/h2]	1	3	0	0	
	[p] Paragraph of text [/p]	1	3	0	1	
170 →	[sec2] DO NOT COPY [/sec2]	1	3	0	2	

22 ↗

Fig. 6

Fig. 7

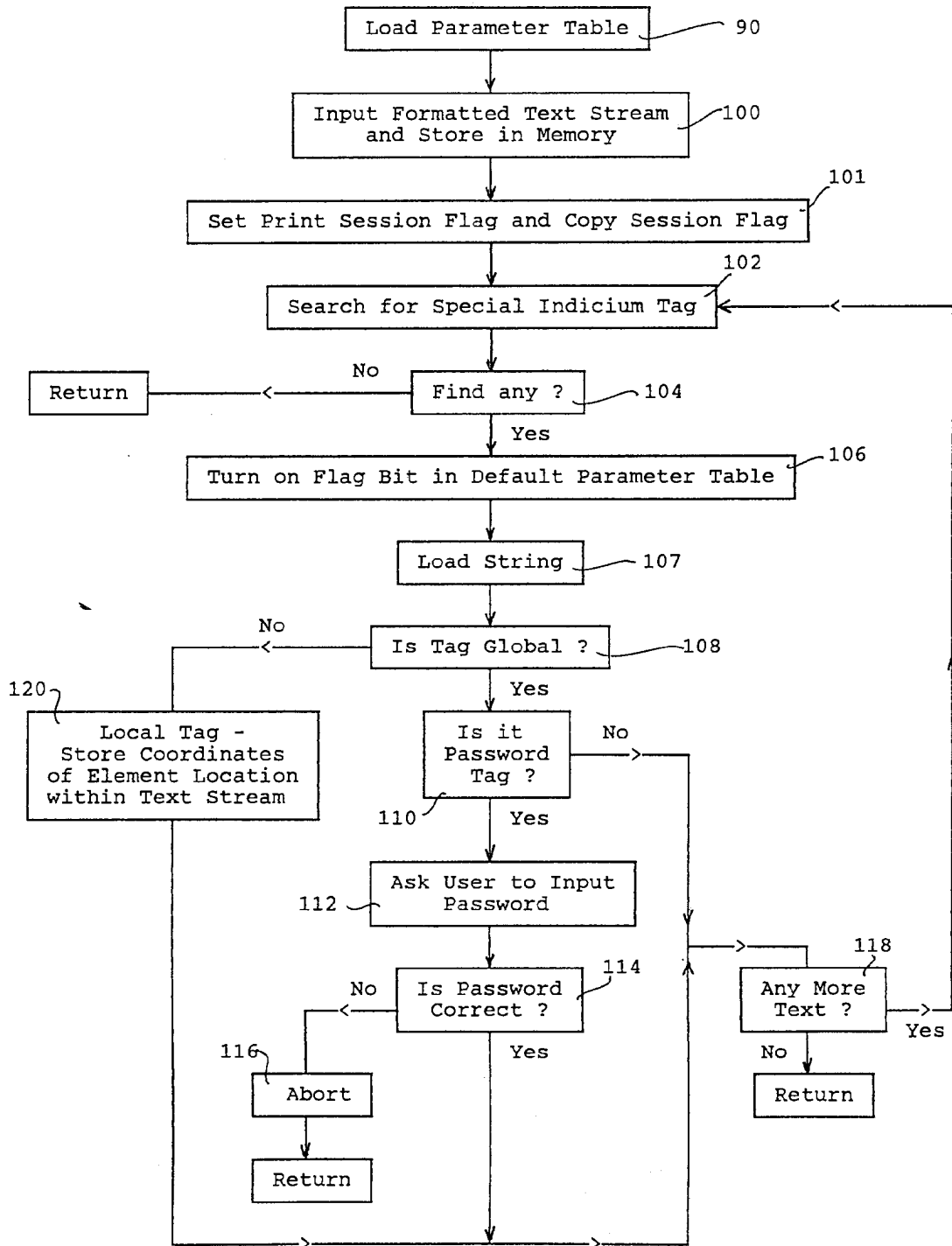
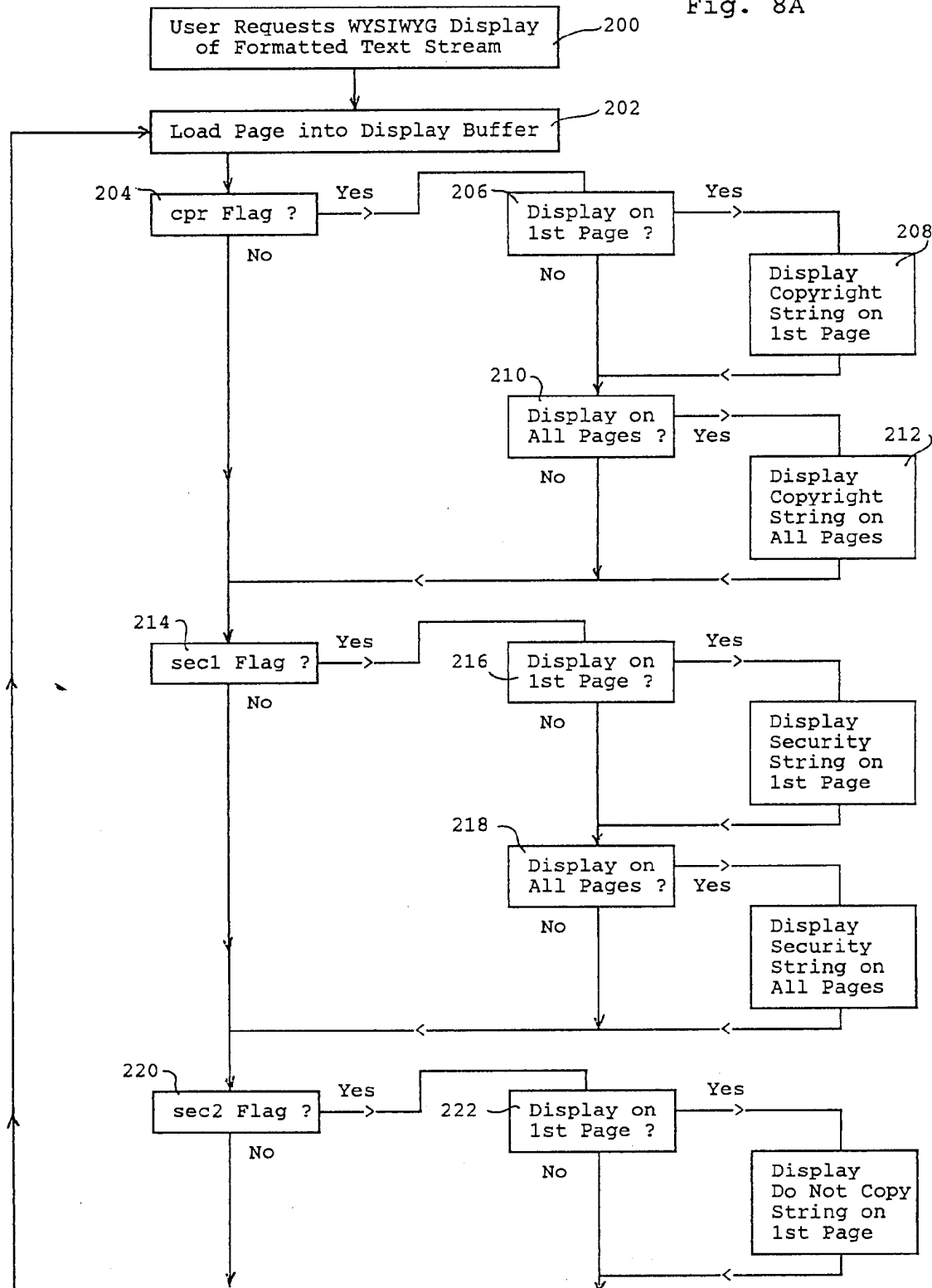


Fig. 8A



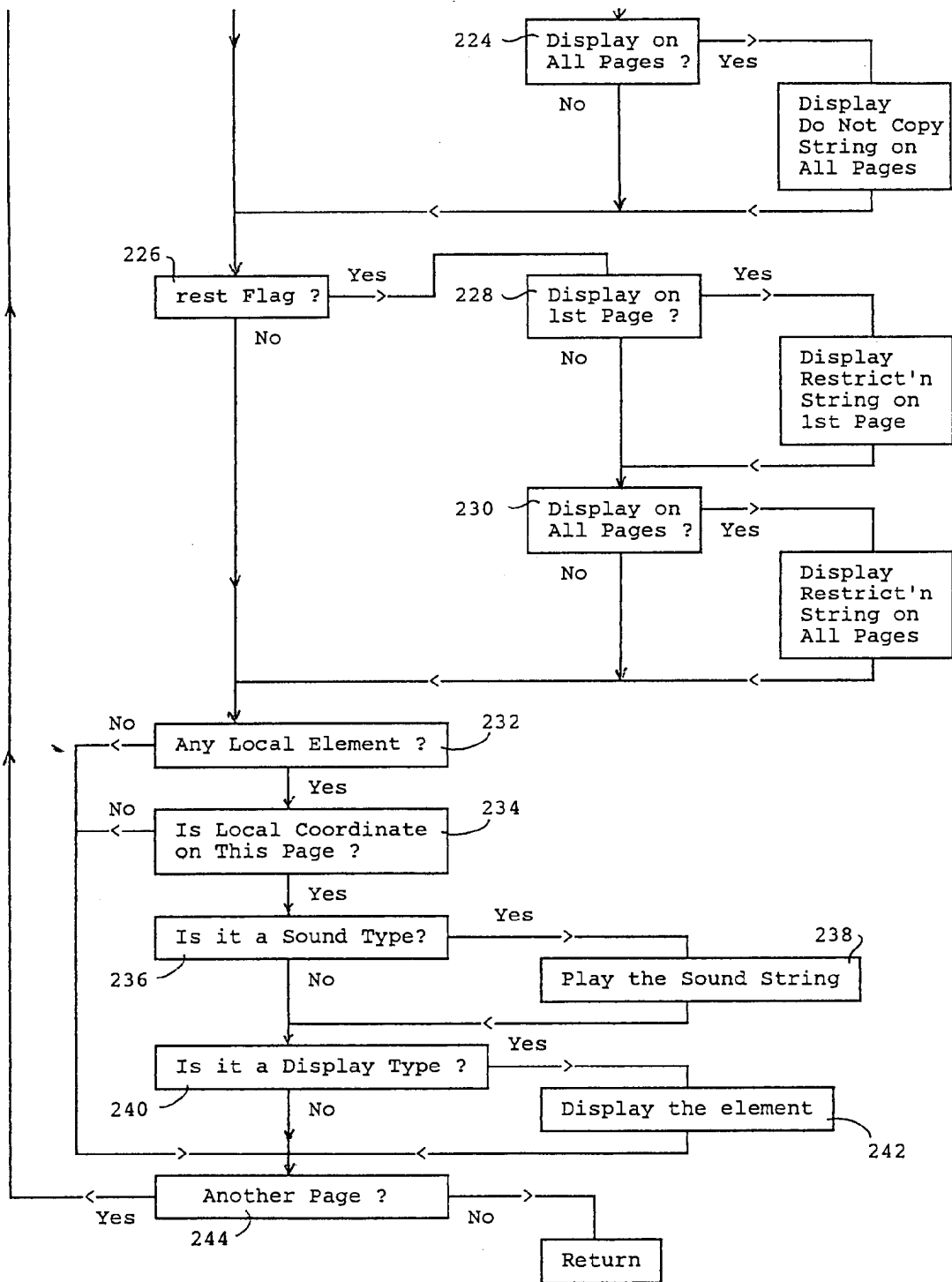


Fig. 8B

Fig. 8

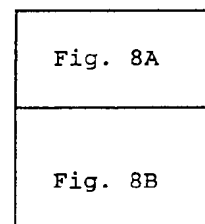
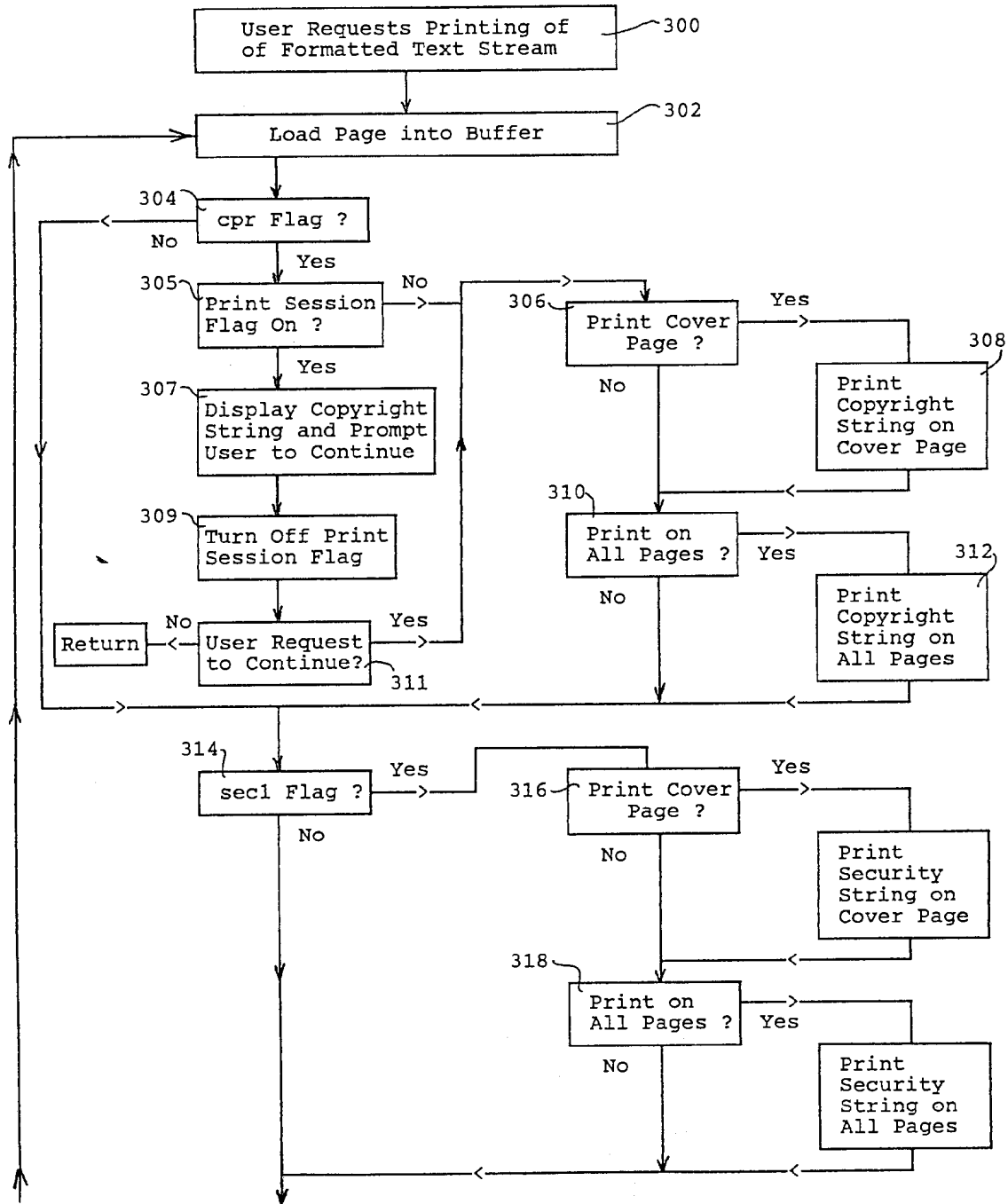


Fig. 9A



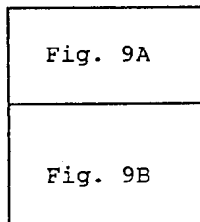
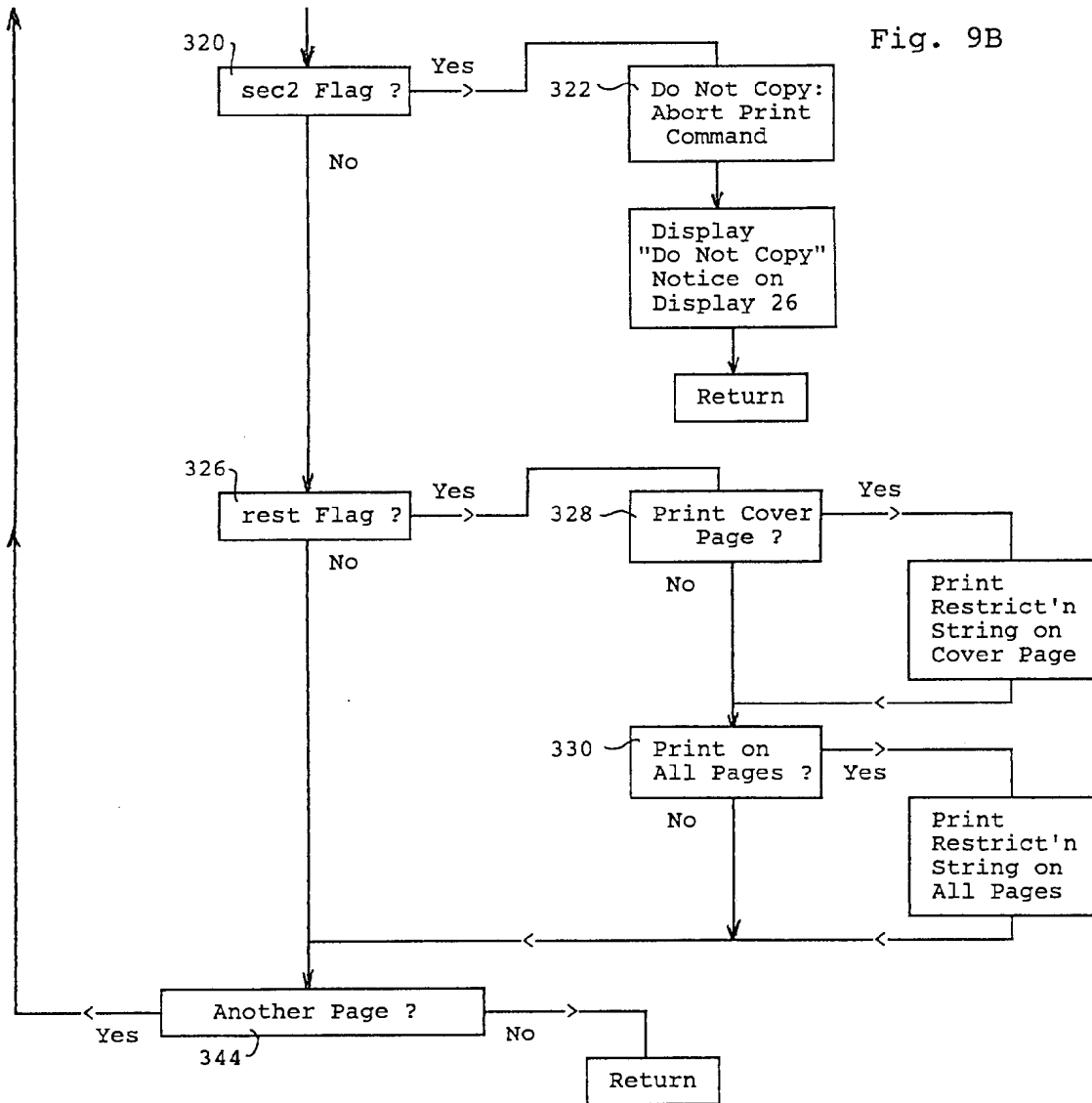


Fig. 9

Fig. 10

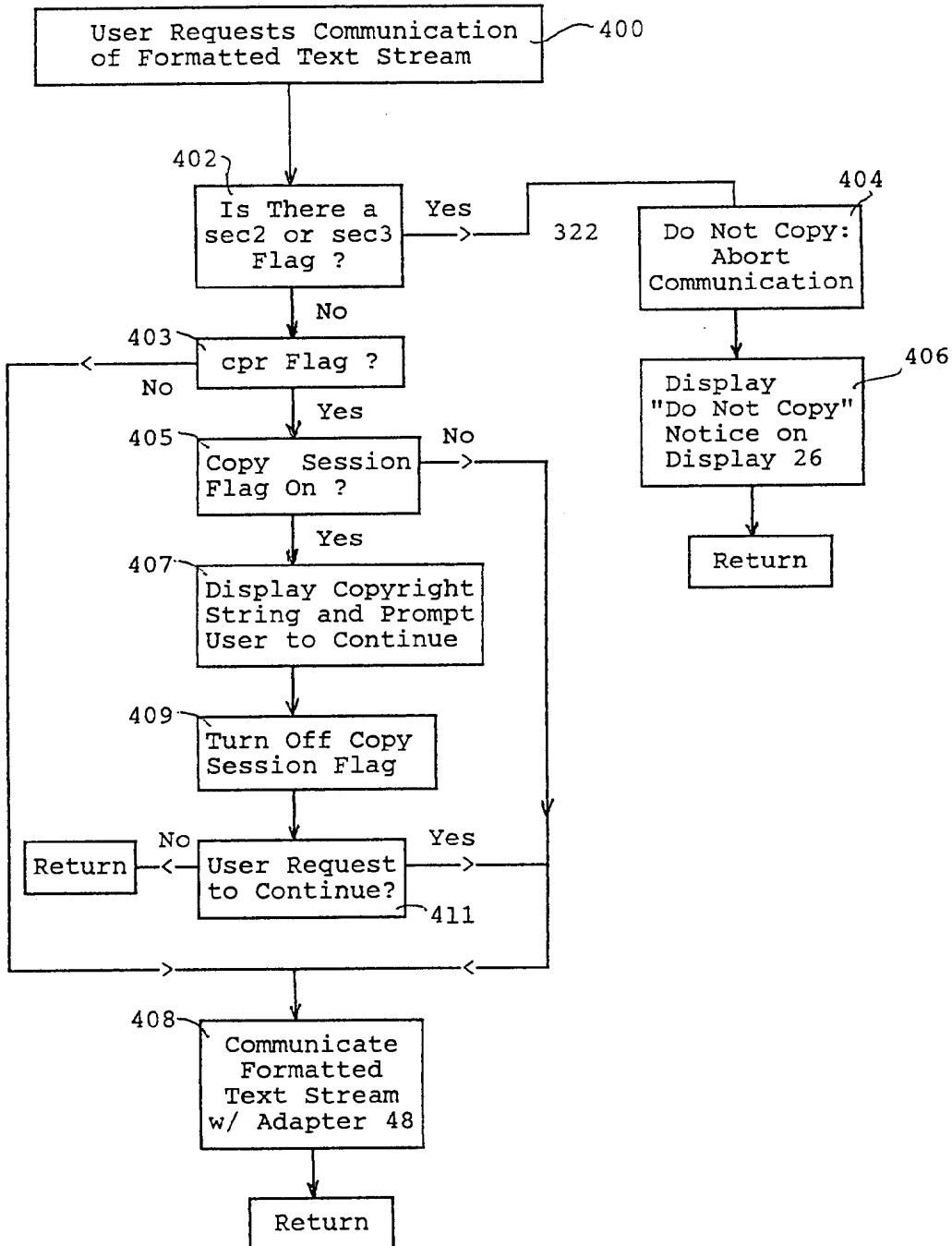
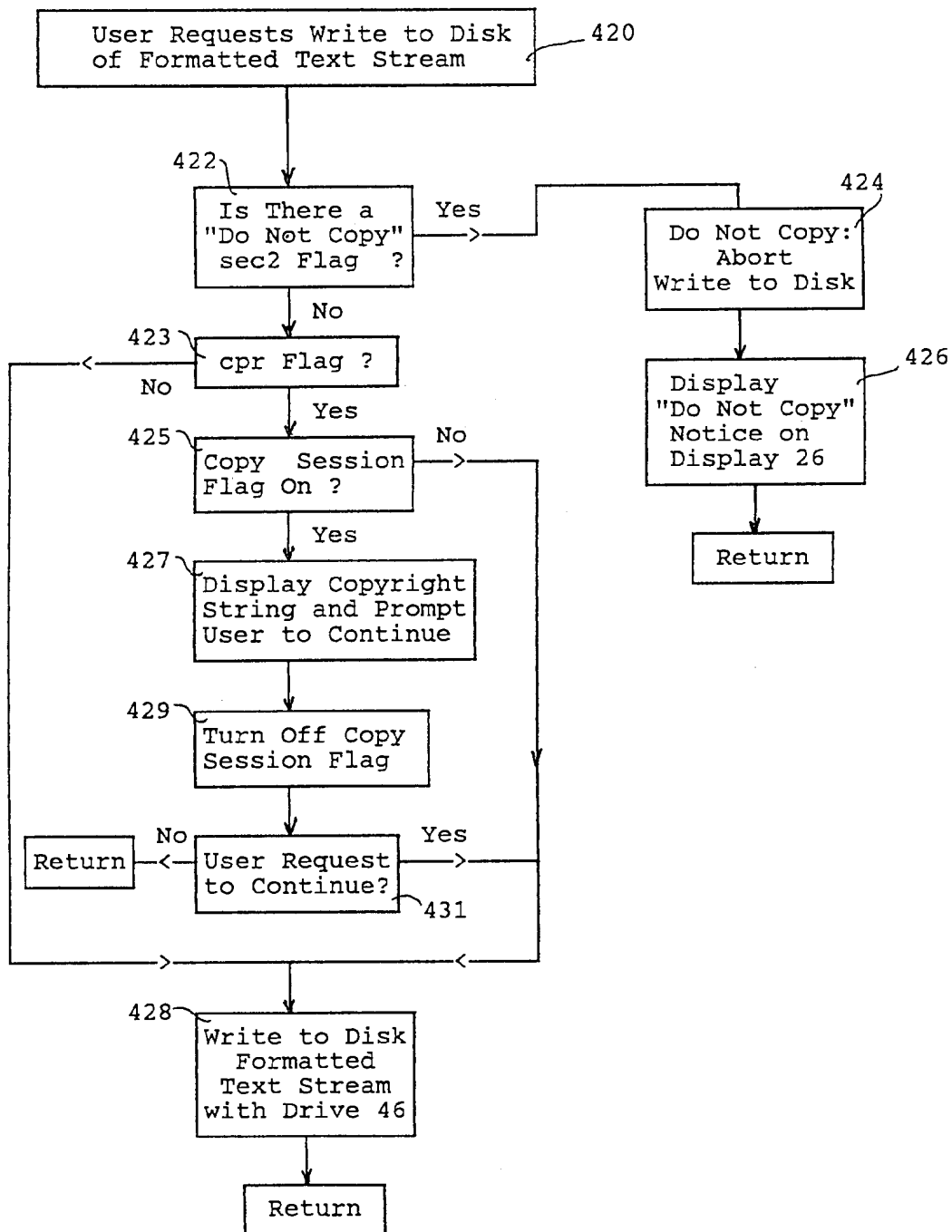


Fig. 11



(19)



Europäisches Patentamt
European Patent Office
Office européen des brevets



(11) Publication number:

0 567 800 A1

(12)

EUROPEAN PATENT APPLICATION(21) Application number: **93105502.4**(51) Int. Cl.5: **G06F 1/00**(22) Date of filing: **02.04.93**(30) Priority: **29.04.92 US 875919**(43) Date of publication of application:
03.11.93 Bulletin 93/44(84) Designated Contracting States:
AT BE CH DE ES FR GB IT LI NL SE(71) Applicant: **INTERNATIONAL BUSINESS MACHINES CORPORATION**
Old Orchard Road
Armonk, N.Y. 10504(US)(72) Inventor: **Hartrick, Thomas Vincent**
170 Sharpstead Lane
Gaithersburg, MD 20878(US)
Inventor: **Stevens, Jeffrey Noel**
18637 Sandpiper Lane
Gaithersburg, MD 20878(US)
Inventor: **Sabia, Nicholas James**
2213 Drury Road
Silver Spring, MD 20906(US)(74) Representative: **Mönig, Anton, Dipl.-Ing.**
IBM Deutschland Informationssysteme GmbH,
Patentwesen und Urheberrecht
D-70548 Stuttgart (DE)(54) **Data processing system and method to enforce payment of royalties when copying softcopy books.**

(57) A publisher of a softcopy book includes royalty payment information either within the structured document text of the book or in a royalty payment information file which accompanies the book. To read the book from the storage disk, the user applies a special softcopy book reading program at his workstation. If the user enters a command to copy the book onto a writable storage medium such as a magnetic disk or to print a hardcopy of the book with a printer or to transmit a copy of the book over a modem, a royalty payment program intercepts the copying command and suspends the copying operations. Instead, the royalty payment program presents the user with a display of the royalty payment information stored in the book text or in a file accompanying the book. The user must select the option of paying a royalty to the publisher before the royalty payment program permits a copy of the book to be made.

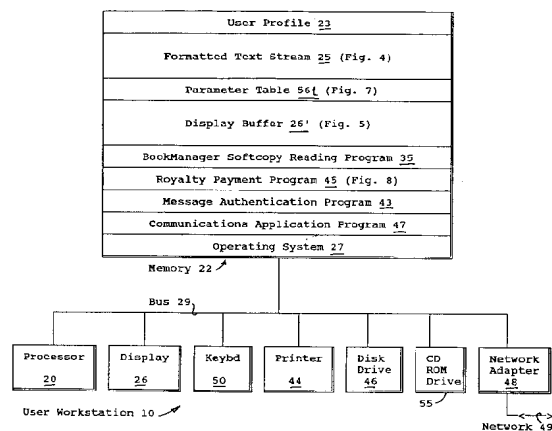


Fig. 1

EP 0 567 800 A1

Technical Field

The invention disclosed broadly relates to data processing and more particularly relates to the management of copying and printing operations for a softcopy document by a data processor, so as to comply with royalty payment requirements for making copies of the document.

Background Art

Modern word processing and text editing programs employ structured document architecture to provide greater control and flexibility in the displayed and printed appearance of documents prepared with the programs. Structured document architecture is described, for example, in the copending U.S. patent application serial number 344,332, filed April 26, 1989, entitled "A Method for Manipulating Elements Within a Structured Document Using Active Intent Interpretation," by C. J. Bennett, D. A. Foulger, E. M. Hesse and D. W. Walsh, assigned to the IBM Corporation and incorporated herein by reference. A structured document can be prepared in accordance with the standardized general markup language, such as is described in the International Standard's Organization Standard 8879-1986. A data stream of text marked up in accordance with the standardized general markup language, will have its text divided into elements consisting of a begin tag and its content and terminated by an end tag, when necessary. Within a WYSIWYG (what you see is what you get) editor, text is displayed to the user as it will appear when it is printed, even though its structure is defined by the begin tags and end tags for each element of text. Formatting of the elements within a structured document is done when the document is displayed to the user. Those elements which fall into the category of commonly used elements include paragraphs, simple lists, ordered lists, bulleted lists, and list items.

Large documents marked up with structured document architecture tags, can be manipulated as a softcopy book, by the method described in the copending U.S. patent application serial number 486,461, filed February 28, 1990, entitled "Method for Associating Annotation With Electronically Published Material" by J. P. DeVries, J. J. Slater, M. E. Moran, J. Unger and E. Cassorla, assigned to the IBM Corporation and incorporated herein by reference. The DeVries, et al. patent application describes a method for creating on-line softcopy books from the same marked up source material used to create printed information such as a word processor or a markup language source used with a text formatter. A book data stream is provided, in an intermediate format for storing on-line informa-

tion, specifically designed to be used by a book display program. The data stream captures and preserves structural information about the books, by using the structured document tags. The method is suited to display on-line softcopy books in a useable manner on a variety of display devices. A book display program manipulates the book data stream and allows users to interact with the on-line information. The electronic book may be used like a hard copy book, except that it is displayed on a display screen. The method allows readers to treat on-line softcopy books as if they were hard copy books, and uses the book data stream as its input.

The book data stream is created by a special softcopy book building program which processes the marked source material by performing a word frequency analysis to form compact data tokens which represent the words in the book. The compacted, tokenized text is then stored as the book data stream on a storage disk such as a compact optical disk. To read the book data stream from the storage disk, a special softcopy book reading program, which reconverts the compacted, tokenized text into the marked source material, which is then capable of being displayed on a display device, copied as an ASCII file onto other storage disks, printed on a hardcopy printer or transmitted over a modem to other data processors. The process for converting the marked source material to the book data stream is described in the US Patent 5,099,426 by R. G. Carlgren and W. D. Modlin, entitled "Method for Use of Morphological Information to Cross Reference Keywords Used for Information Retrieval", assigned to the IBM Corporation and incorporated herein by reference.

The special softcopy book reading program has been embodied in the IBM BookManager (TM) READ program, which helps the user manage, search and look at on-line books. There are two complementary BookManager products, BookManager BUILD is the special softcopy book building program, which creates on-line books from files marked-up with Generalized Markup Language. The BookManager READ product can then manage, search and show the on-line books created by BookManager BUILD. The BookManager READ program product is described in the IBM publication "BookManager (TM) READ, Displaying On-Line Books," publication number SC23-0449-0, February 1989. The BookManager BUILD program product is described in the IBM publication "BookManager (TM) BUILD -Preparing On-Line Books," publication number SC23-0450-0, February 1989. These publications are available from IBM branch offices.

The BookManager BUILD and BookManager READ program products use on-line, softcopy books which are formatted using the Generalized

Markup Language (GML) described in the following two IBM publications: "IBM BookMaster - Text Programmers Notebook -Release 3.0," publication number SC34-5012-02, September 1990 and "IBM BookMaster - Users Guide - Release 3.0," publication number SC34-5009-03, September 1990. Both of these IBM BookMaster publications are available through IBM branch offices.

Softcopy books are frequently communicated, stored, displayed and modified in their softcopy form, with hard copies only occasionally made. Authors of such electronic books or documents frequently desire to impose appropriate forms of security treatment for the electronic books so generated and they wish to have any rights of authorship in their works, respected. This is provided by the invention described in the copending U.S. patent application serial number 546,334, filed June 29, 1990, entitled "Structured Document Tags Invoking Specialized Functions" by T. V. Hartrick, P. E. Higgins and N. J. Sabia, assigned to the IBM Corporation and incorporated herein by reference. The Hartrick, et al. patent application describes a means to enforce the author's intentions for the treatment of his electronic books or documents. The author may place a copyright notice on his softcopy documents, and the mechanism increases the prominence of that notice. Security labels such as "Company Confidential," "Do Not Copy," or "Do Not Distribute," which the author may place on the softcopy of the document, are enforced by limiting or preventing copying.

The invention disclosed by Hartrick, et al. is employed to place a special copyright notice on the first page of the displayed document as it is displayed on the display device. A special structured document tag for copyright which accompanies the copyright notice character string can be located anywhere in the structured document's formatted text stream. This is referred to as a global tag. If a printer is connected to the system and commanded to print the document, a cover page can be selectively printed which includes the copyright notice, before the rest of the structured document is printed by the printer.

Another feature disclosed by Hartrick, et al. is placement of a special "Do Not Copy" label on pages of the document as it is displayed. A special structured document tag accompanies the "Do Not Copy" label in the structured document. Its presence will cause the "Do Not Copy" string, to be selectively displayed on all pages when the document is displayed on the display device. Still further, if a printer connected to the system is commanded to print the document, the printing operation will be aborted in response to the presence of the special structured document tag for the "Do Not Copy" label. Still further, if a disk drive storage

device is connected to the system, a write to disk command for the document will be aborted in response to the special structured document tag for the "Do Not Copy" label. Still further, if a communications adapter is connected to the system, a transmission command for the document will have its function aborted in response to the special structured document tag for the "Do Not Copy" label.

Authors, of course, are in the business of authoring to make money. And this is motivation is not different for those authors and their publishers who have chosen the medium of softcopy books for their publications. What is needed is a means to enforce the payment of royalties to publishers and authors of softcopy books, when a reader desires to make a copy of a portion or all of the book.

Terminology

The following terminology is used in this description, in referring to structured document architecture concepts.

SGML

Standardized General Markup Language. A markup language consisting of tags used to prepare structured documents. Refer to International Standards Organization standard 8879-1986 for definition and details.

Structured document

A document prepared in accordance with an SGML-compliant type definition.

Element

SGML-defined entity consisting of a begin tag and its alphanumeric string content, and including an end tag, when necessary.

Empty element

An element whose contents are null, containing neither text nor other elements.

Current document position

The document position which determines the current page for display.

Commonly used elements

Those elements which fall into the category of commonly used elements include Paragraphs, Simple Lists, Ordered Lists, Bulleted Lists and List

Items.

Tag name

The name given to a set of elements which abide by the same rules of formatting. Examples of a tag name include PARAGRAPH, SIMPLE LIST, and LIST ITEM.

Formatted Text Stream

The formatted text stream is the sequence of alphanumeric characters which includes the structured document tags and associated text for the elements comprising the structured document.

Objects of the Invention

It is therefore an object of the invention to provide an improved method for managing the soft copy text of a structured document in a data processing system, so as to comply with royalty payment requirements of the document.

It is still a further object of the invention to provide an improved method for managing the printing of pages of a structured document, so as to comply with royalty payment requirements of the document.

It is yet another object of the invention to provide an improved method for managing the writing of a structured document into a bulk storage medium, so as to comply with royalty payment requirements of the document.

It is yet a further object of the invention to provide an improved method for managing the telecommunication of soft copies of a structured document, so as to comply with royalty payment requirements of the document.

Summary of the Invention

The author or publisher of a softcopy book specifies the royalty amount he wants to be paid by users who copy the book or individual chapters of the book. The source text of the book has the form of the structured document, formatted text stream.

In accordance with the invention, the publisher includes royalty payment information either within the structured document text of the book or in a royalty payment information file which accompanies the book. The publisher then writes a copy of the book onto a compact disk optical storage medium, a floppy disk magnetic storage medium, or other suitable storage medium. The book is stored on the storage medium as a compacted, tokenized text.

To read the book from the storage disk, the user applies a special softcopy book reading program at his workstation, which reconverts the compacted, tokenized text into the structured document source text, which is then capable of being displayed on a display device.

In accordance with the invention, the user also applies a royalty payment program in conjunction with the softcopy book reading program. If the user enters a command to copy the book onto a writable storage medium such as a magnetic disk or to print a hardcopy of the book with a printer or to transmit a copy of the book over a modem, the royalty payment program intercepts the copying command and suspends the copying operations. Instead, the the royalty payment program presents the user with a display of the royalty payment information stored in the book text or in a file accompanying the book. The user must select the option of paying a royalty to the publisher before the royalty payment program permits a copy of the book to be made.

The royalty payment information contained in the structured document text of the softcopy book or in the royalty information file accompanying the softcopy book, can include royalty payment information on individual chapters of the book, as well as on the entire book. If the user is displaying a particular chapter of the book at his workstation at the time he enters the copying command, the royalty payment program displays royalty payment information for the current chapter being displayed, as well as that for the entire book.

When the user selects to pay the royalty, a communication session is established between the user's workstation and the publisher's data processor, for example by placing a call through a modem and over the public telephone network. A message is sent by the royalty payment program to the publisher's data processor, requesting that the user be permitted to make a copy of a specified part of the book or of the entire book. The request message includes the user's name, his mailing address, and his credit card number or other billing information. The message also contains enough information about the book so that the publisher's data processor can compute the royalty amount the user is to pay.

After checking that the user's offered mode of payment is effective, the publisher's data processor sends back to the user's royalty payment program, an authorization message to make the proposed copy. The royalty payment program in the user's workstation then recommences the copying operation which was suspended, allowing the proposed copy of the book to be made.

The publisher's data processor records the request by the user to make the copy of the book,

and prepares a bill to the user's credit card account.

The authorization message sent by the publisher's data processor in response to the user's request, can contain authentication data which is used by the royalty payment program in the user's workstation to authenticate the authorization message from the publisher. This prevents the user or others from circumventing the royalty payment process.

In accordance with the invention, the authorization message may also contain starting page data which is used in the recovery of aborted copying sessions by the user. As the user is making the proposed copy, an acknowledgement signal is periodically sent from the user's workstation to the publisher's data processor. This is done for each page or chapter successfully copied by the user. The publisher's data processor counts the acknowledgement signals. If the user's copying of the book fails before the proposed copying is completed, then the publisher's data processor stores a fault record with the number of the last page or chapter of the book which was successfully copied. This is indicated by the number of acknowledgement signals received by the publisher. Later, when the user reconnects his workstation with the publisher's data processor and makes another request to copy the book, a new authorization message is sent by the publisher to the user, with the identity of the last page or chapter successfully copied. If the user does not reconnect to the publisher, then the publisher's data processor will bill the user for only the portion of the book which was successfully copied.

The resulting invention provides an improved means to enforce the payment of royalties to publishers and authors of softcopy books, when a reader desires to make a copy of a portion or all of the book.

Brief Description of the Drawings

These and other objects, features and advantages of the invention will be more fully appreciated with reference to the accompanying figures.

Fig. 1 is a system block diagram of the user's workstation, including the royalty payment program, in accordance with the invention.

Fig. 2 is a system block diagram of the publisher's data processor, including the royalty billing program, in accordance with the invention.

Fig. 3A is a first example of element tags and associated text.

Fig. 3B illustrates the memory organization of element tags and associated text, for the first example of Fig. 3A.

Fig. 3C illustrates the appearance of the display of text for the first example of Figs. 3A and 3B.

Fig. 4 is a more detailed diagram of the memory image for a second example of the formatted text stream 25, showing in particular the element coordinates 156 associated with each particular element in the formatted text stream.

Fig. 5 illustrates the appearance of the display of text for the second example of Figs. 4.

Fig. 6 is a diagram of the initially unloaded parameter table 56.

Fig. 7 is a diagram of the parameter table 56 after the it has been loaded with information from elements with special tags.

Figs. 8 and 8A show a flow diagram of the royalty payment program 45.

Fig. 9 is a flow diagram of the royalty billing program 74.

Fig. 10 illustrates the CD ROM 55' which includes the softcopy book and the royalty information file 58, in a second embodiment of the invention.

Fig. 11 shows the display of royalty payment information at the user's workstation.

Description of the Best Mode for Carrying Out the Invention

Fig. 1 is a system block diagram of the user's workstation, including the royalty payment program 45, in accordance with the invention. The workstation 10 includes the processor 20 which is connected by means of the bus 29 to the memory 22. The processor 20 executes program instructions for the programs stored in the memory 22. Also connected to the bus 29 are the display 26, keyboard 50, printer 44, magnetic disk drive 46, compact optical disk drive 55 and the network adapter 48. The network adapter 48 is connected to the communications network 49, which can be the public switched telephone network.

The memory 22 stores User Profile 23, the structured document, formatted text stream 25 (Fig. 4), Loaded Parameter Table 56L (Fig. 7), Display Buffer 26' (Fig. 5), BookManager Softcopy Reading Program 35, Royalty Payment Program 45 (Fig. 8), Communications Application Program 47, and Operating System 27.

The user's workstation is connected over the network 49 to the publisher's data processor 15, as is shown in Fig. 2. The publisher's data processor 15 includes the network adapter 92 which is connected to the network 49 and to the bus 98. Also connected to the bus 98 is the processor 94 and the memory 96. The processor 94 executes program instructions for the programs stored in the memory 96.

The memory 96 stores first book data 70 which includes Total Pages, Chap. 1 Pages and Chap. 2 Pages for the first book. It also stores second book data 72 which includes Total Pages, Chap. 1 Pages, Chap. 2 Pages, and Chap. 3 Pages for the second book. It also stores the Royalty Billing Program 74 (Fig. 9), Publisher's Private Key 76, Public Key Encryption Program 78, Communications Application Program 79, and Operating System 80.

The author or publisher of a softcopy book specifies the royalty amount he wants to be paid by users who copy the book or individual chapters of the book. The source text of the book has the form of the structured document, formatted text stream 25. In accordance with the invention, the publisher includes royalty payment information either within the structured document text of the book or in a royalty payment information file which accompanies the book. Two examples are given of a structured document, formatted text stream which includes royalty payment information, the first example being shown in Figs. 3A, 3B and 3C.

The display device 26 coupled to the processor 20 displays in WYSIWYG form, a plurality of document elements such as paragraphs 28 and 38, the list 30, which includes the list items 32, 34 and 36 shown in the display 26 of Fig. 3C. Cursor 54 is also shown. The elements can include lists which are either ordered or unordered, and elements can also include graphics as well as text. Of special note is the copyright notice 40 and the "Book Reproduction Fee" royalty message 306 displayed in WYSIWYG form for the page of the structured document shown in the display 26 of Fig. 3C. The document elements 28-42 are organized in a formatted text stream having an ordered sequence, as can be seen in Fig. 3A, using structured document notation, where the ordered sequence is specified by a corresponding ordered sequence of the plurality of element tags. The paragraph 28 in Fig. 3A is shown in the structured document notation with the begin tag [p] and the end tag [/p]. Each element such as the paragraph 28 shown in Fig. 3A, is a structured document element having a begin tag [p], the text of the paragraph in this example, and then an end tag [/p]. The begin tag and the end tag serve to identify the element type, in this case indicating a paragraph. The order of occurrence of the WYSIWYG display of paragraph 28 on the display 26 is determined by the order of occurrence in the formatted text stream of the structured document element representing that paragraph 28 shown in Fig. 3A, within the context of the order of occurrence of the other structured document elements, as for example, the list 30 and the paragraph 38.

In accordance with the invention, special strings such as the royalty message 306, are embedded within special elements having special structured document tags in the structured document. Specifically, the royalty message element 306 is a string embedded between a begin tag [royalty] and an end tag [/royalty]. When the processor 20 detects the presence of a special tag such as a royalty begin tag, it makes special note of its presence within the memory 22, so that when specified printer 44, disk drive storage 46, or communications adapter 48 functions are requested, copying is inhibited and a royalty payment process is invoked. For example, if a royalty element 306 is identified in the document text 25, then the printer 44 function will be inhibited if the user requests the printing of the structured document within which the royalty element is identified.

The order of occurrence of the structured document elements such as the paragraph 28, list 30 and paragraph 38, can be determined by their order of occurrence in the formatted text stream stored in the memory 22 as is shown in Fig. 3B. Fig. 3B shows that the structured document text with its tags of Fig. 3A, have been stored in the memory 22 in a linear sequential order, which is the formatted text stream 25. Paragraph element 28 includes tags 28a and 28b and text 28c. List element 30 includes tags 30a and 30b. List item element 32 includes tags 32a and 32b and text 32c. List item element 34 includes tags 34a and 34b and text 34c. List item element 36 includes tags 36a and 36b and text 36c. Paragraph element 38 includes tags 38a and 38b and text 38c.

The special copyright notice element is represented by the begin tag 40a and the end tag 40b which surrounds the copyright notice string 40c. Similarly, the special royalty message "Book Reproduction Fee" element is represented by the begin tag 306a, and the end tag 306b, which surrounds the "Book Reproduction Fee" string 306c. In accordance with the invention, when the processor 20 searches through the formatted text stream 25 stored in the memory 22 and detects the presence of the begin tag 306a or the end tag 306b for the royalty message string 306c, the processor loads the royalty message string 306c into a specified partition 306l of the parameter table 56 shown in Fig. 6 in the memory 22 and it sets a flag 366 or 368 to indicate the presence of a royalty message string, as shown in Fig. 7.

Still further in accordance with the invention, at the time of initial program loading for the royalty payment program 45 into the data processing system shown in Fig. 1, a default parameter table 56 is

loaded into memory at a pre-specified partition. The default parameter table 56 shown in Fig. 6 will have a set of default values entered therein which are stored in the memory 22. Alternately, the user can enter a profile of values for the parameter table 56. The parameter table 56, as loaded at the initial program loading, will include the characters representing each special tag such as the royalty tag "[royalty]" and the like, as is shown in Figs. 6 and 7. Also included in the parameter table 56 of Fig. 6 will be values indicating the response which the data processing system is to make when particular tagged strings are identified in the document text loaded into the memory 22. For example, if a royalty tag "[royalty]" is detected in a structured document, then the default parameter table 56 will indicate that if the document is to be displayed on the display 26, the page displayed will include the royalty message.

Fig. 4 is a more detailed diagram of the memory image for a second example of the formatted text stream 25, showing in particular the paragraph coordinates 156 associated with each particular paragraph, heading and other element in the formatted text stream 25. The formatted text stream 25 illustrated in Fig. 4 has structured document tags similar to those referenced above. The structured document of Fig. 4 is shown as it is displayed in WYSIWYG form on the display 26 of Fig. 5. The structured document 25 of Fig. 4 has three major parts, the book title portion consisting of elements 300 to 314, the first chapter portion consisting of elements 316 to 340, and the second chapter portion consisting of elements 342 to 350.

The book title portion of the second example document 25 of Fig. 4, has the following elements: "[bk] Book Title [bk]" 300, "[ed] Second Edition [ed]" 302, "[cpr] (C) ABC Co 1990 [cpr]" 304, "[royalty] Book Reproduction Fee [/royalty]" 306, "[amount] \$20.00 [/amount]" 308, "[phone] 1-800-123-1234 [/phone]" 310, "[public key] 13A723F9...6 [/public key]" 312, and "[validation] The Book Repro Fee Is Paid [/validation]" 314.

Royalty message 306 is represented by the special tag [royalty] followed by the special royalty message string "Book Reproduction Fee" and followed by the end tag [/royalty]. The default table 56 column 364 of Fig. 7 shows that this string will be displayed on the display 26. When a royalty element such as 306, is the first to occur in a structured document 25 and it does not occur within a chapter heading such as [h1], it is considered a global element which is given effect for the entire book. It is flagged in the book royalty flag column 366 of the default table 56 of Fig. 7. Since royalty element 306 is the first occurring royalty

element in the structured document 25, it represents the royalty message for copying the entire book. The associated royalty information in the special elements which occur immediately following royalty message 306 are also considered global elements which apply when the entire book is to be copied. The associated elements to royalty element 306 are "[amount] \$20.00 [/amount]" 308, "[phone] 1-800-123-1234 [/phone]" 310, "[public key] 13A723F9...6 [/public key]" 312, and "[validation] The Book Repro Fee Is Paid [/validation]" 314.

The element "[amount] \$20.00 [/amount]" 308 represents the charge for copying the entire book. The default table 56 column 364 of Fig. 7 shows that this string will be displayed on the display 26.

The element "[phone] 1-800-123-1234 [/phone]" 310 represents the phone number of the publisher's data processor 15, which is called over the telephone network 49. The default table 56 column 364 of Fig. 7 shows that this string will be displayed on the display 26.

The element "[public key] 13A723F9...6 [/public key]" 312 is the publisher's public key which the user's royalty payment program 45 uses to validate that the authorization message received from the publisher is authentic. The default table 56 column 364 of Fig. 7 shows that this string will not be displayed on the display 26.

The element "[validation] The Book Repro Fee Is Paid [/validation]" 314, is the string which the user's royalty payment program 45 compares with the publisher's authorization message to insure that it is authentic. The default table 56 column 364 of Fig. 7 shows that this string will not be displayed on the display 26.

The first chapter portion of the second example document 25 of Fig. 4, has the following elements:

"[h1] First Chapter Heading [/h1]" 316,
 "[royalty] Chapter Reproduction Fee [/royalty]" 318,
 "[amount] \$ 1.00 [/amount]" 320,
 "[validation] First Chapter Fee Paid [/validation]" 322,
 "[p] Paragraph of text [/p]" 324,
 "[h2] First topic heading [/h2]" 326,
 "[p] Paragraph of text [/p]" 328,
 "[p] Paragraph of text [/p]" 330,
 "[h2] Second topic heading [/h2]" 332,
 "[p] Paragraph of text [/p]" 334,
 "[h3] First subtopic heading [/h3]" 336,
 "[p] Paragraph of text [/p]" 338, and
 "[p] Paragraph of text [/p]" 340,

The structured document tags for the first chapter heading is the begin tag [h1] and the end tag [/h1]. Under the chapter heading, there are four elements, the first being a royalty message 318 represented by the special tag [royalty] followed by

the special royalty message string "Chapter Reproduction Fee" and followed by the end tag [/royalty]. The default table 56 column 364 of Fig. 7 shows that this string will be displayed on the display 26. When a royalty element occurs within a chapter heading such as [h1], it is considered a local element which is given effect only within the chapter h1. It is flagged in the chapter royalty flag column 368 of the default table 56 of Fig. 7. Since royalty element 318 is the second occurring royalty element in the structured document 25, occurring after the royalty element 306, it is not substituted for the book royalty element 306.

The associated royalty information in the special elements which occur immediately following royalty message 318 are also considered local elements which apply only to the first chapter when it is to be copied. The associated elements to royalty element 318 are "[amount] \$ 1.00 [/amount]" 320, and "[validation] First Chapter Fee Paid [/validation]" 322.

The second element is a royalty amount 320 represented by the special tag [amount] followed by the special royalty amount string "\$ 1.00" and followed by the end tag [/amount]. The default table 56 column 364 of Fig. 7 shows that this string will be displayed on the display 26.

The third element is a validation datum 322 represented by the special tag [validation] followed by the special validation string "First Chapter Fee Paid" and followed by the end tag [/validation]. The default table 56 column 364 of Fig. 7 shows that this string will not be displayed on the display 26.

The fourth element under the chapter heading is a paragraph element 324 denoted by a paragraph begin tag [p] and an end tag [/p].

The formatted text stream 25 is characterized by a hierarchical organization, in that the first topic heading element 326 depicted by its begin tag [h2] and end tag [/h2], is subsidiary to the chapter heading element 316 in the hierarchy. Use is made of this hierarchical structure for the formatted text stream 25, to establish a coordinate system 156.

The coordinate system 156 is shown in Fig. 4 as it can be stored in memory 22, with six digits representing the hierarchical level of the particular heading or element entry to which the coordinate is associated. For example, the paragraph element 330 has a coordinate of bk=1, h1=1, h2=1, h3=0, p=2 and e1=1. This means that the element 330 is part of the first book bk=1, part of the first h1 chapter heading, part of the first h2 topic heading, and is not part of any subsidiary topic heading to the first topic heading. The p=2 coordinate represents that element 330 is the second paragraph element under the first topic heading. The e1=1 coordinate represents that the element 330 is the first element in the paragraph.

The second chapter portion of the second example document 25 of Fig. 4, has the following elements:

"[h1] Second Chapter Heading [/h1]" 342,
 "[royalty] Chapter Reproduction Fee [/royalty]" 344,
 "[amount] \$ 2.00 [/amount]" 346,
 "[validation] Second Chapter Fee Paid [/validation]" 348, and
 "[p] Paragraph of text [/p]" 350.

The structured document tags for the second chapter heading 342 is the begin tag [h1] and the end tag [/h1]. Under the chapter heading 342, there are four elements, the first being a royalty message 344 represented by the special tag [royalty] followed by the special royalty message string "Chapter Reproduction Fee" and followed by the end tag [/royalty]. The default table 56 column 364 of Fig. 7 shows that this string will be displayed on the display 26. When a royalty element occurs within a chapter heading such as 342, it is considered a local element which is given effect only within the second chapter 342. It is flagged in the chapter royalty flag column 368 of the default table 56 of Fig. 7. Since royalty element 344 is the third occurring royalty element in the structured document 25, occurring after the royalty elements 306 and 318, it is not substituted for the book royalty element 306.

The associated royalty information in the special elements which occur immediately following royalty message 344 are also considered local elements which apply only to the second chapter when it is to be copied. The associated elements to royalty element 344 are "[amount] \$ 2.00 [/amount]" 346, and "[validation] Second Chapter Fee Paid [/validation]" 348.

The second element is a royalty amount 346 represented by the special tag [amount] followed by the special royalty amount string "\$ 2.00" and followed by the end tag [/amount]. The default table 56 column 364 of Fig. 7 shows that this string will be displayed on the display 26.

The third element is a validation datum 348 represented by the special tag [validation] followed by the special validation string "Second Chapter Fee Paid" and followed by the end tag [/validation]. The default table 56 column 364 of Fig. 7 shows that this string will not be displayed on the display 26.

The fourth element under the chapter heading is a paragraph element 350 denoted by a paragraph begin tag [p] and an end tag [/p].

The author or publisher of a softcopy book specifies the royalty amount he wants to be paid by users who copy the book or individual chapters of the book. The source text of the book has the form of the structured document, formatted text

stream 25. In accordance with the invention, the publisher includes royalty payment information either within the structured document text of the book or in a royalty payment information file which accompanies the book.

In accordance with the invention, the publisher includes royalty payment information either within the structured document text of the book as shown in Fig. 4 or in a royalty payment information file 58 which accompanies the book, as shown in Fig. 10. The publisher then writes a copy of the book onto a compact disk optical storage medium, a floppy disk magnetic storage medium, or other suitable storage medium, 55'. The book is stored on the storage medium as a compacted, tokenized text.

To read the book from the storage disk, the user applies a special softcopy book reading program 35, at his workstation 10, which reconverts the compacted, tokenized text into the structured document source text, which is then capable of being displayed on a display device 26, as shown in Fig. 5.

In accordance with the invention, the user also applies a royalty payment program 45 of Fig. 8 in conjunction with the softcopy book reading program 35. If the user enters a command to copy the book onto a writable storage medium such as a magnetic disk on disk drive 46 or to print a hard-copy of the book with a printer 44 or to transmit a copy of the book over a modem and network adapter 48, the royalty payment program 45 intercepts the copying command and suspends the copying operations.

Instead, the the royalty payment program 45 presents the user with a display of the royalty payment information stored in the book text of Fig. 4 or in the file 58 accompanying the book. The user must select the option of paying a royalty to the publisher before the royalty payment program permits a copy of the book to be made.

The royalty payment information contained in the structured document text 25 of the softcopy book shown in Fig. 4 or in the royalty information file 58 accompanying the softcopy book, can include royalty payment information on individual chapters of the book, as well as on the entire book. If the user is displaying a particular chapter of the book at his workstation at the time he enters the copying command, the royalty payment program 45 displays royalty payment information for the current chapter being displayed, as well as that for the entire book, as is shown in Fig. 11.

When the user selects to pay the royalty, a communication session is established between the user's workstation 10 and the publisher's data processor 15, for example by placing a call through a modem and network adapter 48 and over the public telephone network 49. A message is sent by the

royalty payment program 45 to the publisher's data processor 15, requesting that the user be permitted to make a copy of a specified part of the book or of the entire book. The request message includes the user's name, his mailing address, and his credit card number or other billing information. The message also contains enough information about the book so that the publisher's data processor can compute the royalty amount the user is to pay.

The publisher's data processor 15 has a royalty billing program 74, shown in Fig. 9, which receives and processes the user's request message. After checking that the user's offered mode of payment is effective, the royalty billing program 74 in the publisher's data processor 15, sends back to the user's royalty payment program 45, an authorization message to make the proposed copy. The royalty payment program 45 in the user's workstation 10 then recommences the copying operation which was suspended, allowing the proposed copy of the book to be made.

The royalty billing program 74 in the publisher's data processor 15 records the request by the user to make the copy of the book, and prepares a bill to the user's credit card account.

The authorization message sent by the royalty billing program in the publisher's data processor 15 in response to the user's request, can contain authentication data which is used by the royalty payment program 45 in the user's workstation 10 to authenticate the authorization message from the publisher. This prevents the user or others from circumventing the royalty payment process.

In accordance with the invention, the authorization message may also contain starting page data which is used in the recovery of aborted copying sessions by the user. As the user is making the proposed copy, an acknowledgement signal is periodically sent from the user's workstation 10 to the publisher's data processor 15, as shown in Fig. 8. This is done for each page or chapter successfully copied by the user. The royalty billing program 74 in the publisher's data processor 15 counts the acknowledgement signals, as shown in Fig. 9. If the user's copying of the book fails before the proposed copying is completed, then the royalty billing program 74 in the publisher's data processor 15, stores a fault record with the number of the last page or chapter of the book which was successfully copied. This is indicated by the number of acknowledgement signals received by the publisher's royalty billing program 74. Later, when the user reconnects his workstation 10 with the publisher's data processor 15 and makes another request to copy the book, a new authorization message is sent by the publisher's royalty billing program 74 to the user's royalty payment program 45, with the identity of the last page or chapter suc-

cessfully copied. If the user does not reconnect his workstation 10 to the publisher's data processor 15, then the royalty billing program 74 in the publisher's data processor 15 will bill the user for only the portion of the book which was successfully

copied. As was discussed above, the authorization message sent by the royalty billing program 74 in the publisher's data processor 15 in response to the user's request, can contain authentication data which is used by the royalty payment program 45 in the user's workstation 10 to authenticate the authorization message received from the publisher. The authentication data can be as simple as the publisher's royalty billing program 74 sending back a data word which is compared at the workstation 10 with a similar data word retained by the user's royalty payment program 45. Alternately, a more sophisticated authentication technique can be employed, such as the publisher's royalty billing program 74 applying a digital signature to the authorization message, which can be authenticated by the user's royalty payment program 45. The standard technique for applying a digital signature to authenticate a message is by use of a public key encryption algorithm.

Public key encryption algorithms are described in a paper by W. Diffie and M. E. Hellman entitled "Privacy and Authentication: An Introduction to Cryptography," Proceedings of the IEEE, Volume 67, No. 3, March 1979, pp. 397-427. Public key systems are based on dispensing with the secret key distribution channel, as long as the channel has a sufficient level of integrity. In a public key cryptographic system, two keys are used, one for enciphering and one for deciphering. Public key algorithm systems are designed so that it is easy to generate a random pair of inverse keys PU for enciphering and PR for deciphering and it is easy to operate with PU and PR, but is computationally infeasible to compute PR from PU. Each communicating party generates a pair of inverse transforms, PU and PR. The party keeps the deciphering transformation PR secret, and makes the enciphering transformation PU public by placing it in a public directory. Anyone can now encrypt messages and send them to the party, but no one else can decipher messages intended for him. It is possible, and often desirable, to encipher with PU and decipher with PR. For this reason, PU is usually referred to as a public key and PR is usually referred to as a private key.

A corollary feature of public key cryptographic systems is the provision of a digital signature which uniquely identifies the sender of a message. If party A wishes to send a signed message M to party B, party A operates on it with his private key PR to produce the signed message S. PR was

used as party A's deciphering key when privacy was desired, but it is now used as his "enciphering" key to send a digital signature. When party B receives the message S, he can recover the message M by operating on the ciphertext S with party A's public PU. By successfully decrypting party A's message, the receiver B has conclusive proof it came from the sender A. Digital signatures can be produced either by encrypting the data to be signed with the private key, which works well when the data is short, or by first hashing the data with a strong one-way cryptographic function and encrypting the so-produced hashed value with the private key. Either method will work.

A method for producing digital signatures based on the hash of the data to be signed is taught in co-pending US Patent Application by S. M. Matyas, et al., "A Hybrid Public Key Algorithm/Data Encryption Algorithm Key Distribution Method Based on Control Vectors," serial number 07/748,407, filed August 22, 1991, assigned to IBM Corporation and incorporated herein by reference.

Examples of public key cryptography are provided in the following U.S. patents: USP 4,218,582 to Hellman, et al., "Public Key Cryptographic Apparatus and Method;" USP 4,200,770 to Hellman, et al., "Cryptographic Apparatus and Method;" and USP 4,405,829 to Rivest, et al., "Cryptographic Communications System and Method."

The public key encryption technique is applied to appending the publisher's digital signature to the authorization message sent from the publisher's royalty billing program 74 to the user's royalty payment program 45. The publisher initially creates a public key and a corresponding private key 76, as discussed above. The publisher's public key is inserted as the public key element 312 into the formatted text stream 25 of the softcopy book of Fig. 4. The publisher then publishes the softcopy book on a CD ROM medium, which the user buys. In an alternate embodiment, the publisher's public key is included in the royalty information file 58 on the CD ROM 55' of Fig. 10.

When the user inputs a command to make a copy of the book, the user's royalty payment program 45 sends a copy of the validation string 314 to the publisher, along with his request to copy the book. If the request is to copy one chapter, such as the first chapter, then the validation string 322 for that chapter is sent to the publisher with the request. The publisher's royalty billing program 74 then operates on the validation string it receives from the user, by encrypting the string with the publisher's private key 76, using the public key encryption program 78. The publisher's royalty billing program 74 then sends the encrypted validation

string back to the user as part of the authorization message.

The user's royalty payment program 45 then operates on the encrypted validation string it receives from the publisher, by decrypting it with the publisher's public key obtained from the public key element 312 contained in the softcopy book. The user's royalty payment program 45 uses a message authentication program 43 which includes the public key encryption algorithm referred to above, to perform the decryption. The decrypted validation string is then compared with the validation string 314 or 322 contained in the softcopy book. If the comparison is satisfied, then only the publisher's royalty billing program 74 could have sent the authorization message.

Figs. 8 and 8A show a flow diagram of the royalty payment program 45, which is executed in the user's workstation 10.

Fig. 8 starts with step 400, Begin BookManager Softcopy Book Reader Program 35.

Then in step 402, Begin Royalty Payment Program 45.

Then in step 404, Input formatted text stream 25 and store in memory 22.

Then in step 406, Search for elements with special tags 360 (Fig. 6).

Then in step 408, Load text strings 362 and element coordinates 156 for elements with special tags 360, into parameter table 56L (Fig. 7).

Then in step 410, Set book royalty flag 366 in table 56L (Fig. 7).

Then in step 412, Set chapter royalty flags 368 in table 56L (Fig. 7).

Then in step 414, Continue with BookManager Softcopy Book Reader Program 35.

Then in step 416, Detect user input request to print or copy.

Then in step 418, Identify chapter of book being viewed.

Then in step 420, Display heading of chapter being reviewed 342, chapter royalty payment message 344 and chapter payment amount 346 (Fig. 11).

Then in step 422, Display title of book 300, book royalty payment message 306 and book payment amount 308 (Fig. 11).

Then in step 424, Prompt user to enter selection (Fig. 11).

Then in step 426, Get user profile 23, including user's name, mailing address and credit card information.

Then in step 428, Get phone number 310 of publisher's data processor 15.

Then in step 430, Place telephone call to publisher's data processor 15 using communications application program 47.

Then in step 432, Send request to publisher to print or copy, including user profile 23, book title 300, edition 302 and amount 308, user's chapter or book selection, and validation string 348.

Then in step 434, Receive authorization message from publisher's processor 15, including validation string encrypted with publisher's private key, and the START_PAGE value.

Then in step 436, Decrypt the encrypted validation string with publisher's public key 312, using the public key encryption algorithm in the message authentication program 43.

Then in step 438, If the decrypted validation string from the publisher compares with the validation string 348, then enable the printer 44 to print or the disk drive 46 to copy the selected chapter or book, beginning at the START_PAGE value.

Then in step 440, Send an ACK acknowledgment to the publisher's processor 15 when each page of the selection is successfully printed or copied.

Then in step 442, Optionally print the publisher's authorization message on the copy.

Then in step 444, Return to the BookManager Softcopy Book Reader Program 35.

Fig. 9 is a flow diagram of the royalty billing program 74, which is executed in the publisher's data processor 15.

Fig. 9 starts with step 500, Begin Royalty Billing Program 74.

Then in step 501, Receive request from user workstation 10 to print or copy, including user profile 23, book title 300, edition 302 and amount 308 user's chapter or book selection, and validation string 348.

Then in step 502, Check user's credit.

Then in step 504, Get book data 70.

Then in step 505, If there is a fault record for this user and book, then set START_PAGE = page where stopped in fault record, else set START_PAGE = 1.

Then in step 506, Encrypt validation string with publisher's private key 76.

Then in step 508, Assemble authorization message including validation string encrypted with publisher's private key 76, and the START_PAGE value.

Then in step 510, Send authorization message to user's workstation 10.

Then in step 512, Get number of pages MAX_PAGE to be copied, from book data 70.

Then in step 514, Compute PER_PAGE charge, Set BILL = 0 and PAGE = START_PAGE.

Then in step 516, Receive ACK from user workstation 10.

Then in step 518, BILL = BILL + PER_PAGE: PAGE = PAGE + 1.

Then in step 520, If there are more ACKs, then goto step 516, else goto step 522.

Then in step 522, If PAGE < MAX_PAGE, then create a fault record, including user profile 23, book title 300, edition 302 and amount 308, user's chapter or book selection, and value of PAGE where copying failed.

Then in step 524, Print invoice to user with amount charged = BILL.

Then in step 526, Return to the main program.

Fig. 10 illustrates the CD ROM 55' which includes the softcopy book Formatted Text Stream 25 and the royalty information file 58, in a second embodiment of the invention.

Fig. 11 shows the display of royalty payment information at the user's workstation. In this example, two options are presented to the user for selection. The first is for "Reproduction Fees For Current Chapter Being Viewed". The example shown is for "Second Chapter Heading". The user may select this option by typing an "X" in the box. Alternately, the user may use a pointing device such as a mouse, to make the selection. The second option is for "Reproduction Fees For The Entire Book Being Viewed. For this option "Book Title", "Second Edition", and "Book Reproduction Fee" are displayed and can be selected in the same manner. The resulting invention provides an improved means to enforce the payment of royalties to publishers and authors of softcopy books, when a reader desires to make a copy of a portion or all of the book.

Although a specific embodiment of the invention has been disclosed, it will be understood by those having skill in the art that changes can be made to the specific embodiment without departing from the spirit and the scope of the invention.

Claims

1. A method for managing the printing of pages of a structured document on a printer device in a network, so as to comply with royalty payment requirements of the document, comprising the steps of:

inputting into a first data processor in said network, a formatted text stream of a structured document which includes a royalty payment element having a special tag;

searching said formatted text stream to identify said royalty payment element and storing a royalty payment flag in a memory in said first data processor;

receiving a command from a user to print a portion of said document on a printer device controlled by said first data processor;

transmitting from said first data processor to a second data processor in said network, a re-

quest for authorization to print said portion of said document, in response to said print command and to said royalty payment flag;

receiving said request at said second data processor and in response thereto, charging said user a royalty payment amount;

transmitting from said second data processor to said first data processor an authorization message for printing said portion of said document;

receiving said authorization message at said first data processor and in response thereto, outputting a print control signal from said first data processor to said printer to print said portion of said document on said printer device.

2. A method for managing the copying of pages of a structured document on a copying device in a network, so as to comply with royalty payment requirements of the document, comprising the steps of:

inputting into a first data processor in said network, a formatted text stream of a structured document which includes a royalty payment element having a special tag;

searching said formatted text stream to identify said royalty payment element and storing a royalty payment flag in a memory in said first data processor;

receiving a command from a user to copy a portion of said document on a copying device controlled by said first data processor;

transmitting from said first data processor to a second data processor in said network, a request for authorization to copy said portion of said document, in response to said copy command and to said royalty payment flag;

receiving said request at said second data processor and in response thereto, charging said user a royalty payment amount;

transmitting from said second data processor to said first data processor an authorization message for copying said portion of said document;

receiving said authorization message at said first data processor and in response thereto, outputting a copy control signal from said first data processor to said copying device to copy said portion of said document on said copying device.

3. A method for managing the communicating of pages of a structured document on a communicating device in a network, so as to comply with royalty payment requirements of the document, comprising the steps of:
 - inputting into a first data processor in said

network, a formatted text stream of a structured document which includes a royalty payment element having a special tag;
 searching said formatted text stream to identify said royalty payment element and storing a royalty payment flag in a memory in said first data processor;
 receiving a command from a user to communicate a portion of said document on a communicating device controlled by said first data processor;
 transmitting from said first data processor to a second data processor in said network, a request for authorization to communicate said portion of said document, in response to said communicate command and to said royalty payment flag;
 receiving said request at said second data processor and in response thereto, charging said user a royalty payment amount;
 transmitting from said second data processor to said first data processor an authorization message for communicating said portion of said document;
 receiving said authorization message at said first data processor and in response thereto, outputting a communicate control signal from said first data processor to said communicating device to communicate said portion of said document on said communicating device.

4. The method of claim 1, 2 or 3, which further comprises:
 said formatted text stream including royalty payment information;
 including said royalty payment information in said request for authorization, or/and which further comprises:
 said step of inputting a formatted text stream further comprising:
 reading a file containing said formatted text stream, from a storage medium coupled to said first data processor;
 said storage medium further including an address file containing a network address for said second data processor;
 said step of transmitting said request for authorization from said first data processor to a second data processor in said network, further comprising:
 reading said address file to access said network address of said second data processor, or/and which further comprises:
 said step of transmitting said request for authorization from said first data processor to a second data processor in said network, further comprising:
 assembling document identity data for said

document, portion specification data for said portion to be copied, and user identity data for said user;
 including said document identity data, said portion specification data, and said user identity data in said request for authorization, or/and which further comprises:
 said step of inputting a formatted text stream further comprising:
 reading a file containing said formatted text stream, from a storage medium coupled to said first data processor;
 said storage medium further including a validation file containing validation data for said second data processor;
 said step of transmitting an authorization message from said second data processor to said first data processor, further comprising the steps of:
 transmitting sender identity data which identifies said second data processor as the actual sender of said authorization message;
 reading said validation file to access said validation data at said first data processor;
 said step of receiving said authorization message at said first data processor further comprising:
 validating that said second data processor is the actual sender of said authorization message by processing said sender identity data with said validation data at said first data processor, or/and which further comprises:
 said step of validating is by means of comparing said sender data with said validation data.

5. The method of claim 1, 2, 3 or 4, which further comprises:
 said validation data is a public key, of a public key, private key pair, issued by said second data processor;
 said sender identity data is an encrypted message, encrypted by said second data processor under said private key;
 said step of validating is by means of decrypting said encrypted message using said public key at said first data processor.
6. The method of any one of the claims 1 to 5, which further comprises:
 said step of outputting a communicate control or copy control or print control signal from said first data processor, further comprising:
 outputting a first acknowledgement signal from said first data processor to said second data processor when a first fraction of said portion of said document has been copied by said communicating device or has been copied by said copying device or has been printed by

said printer;
 outputting a second acknowledgement signal
 from said first data processor to said second
 data processor when a second fraction of said
 portion of said document has been copied by 5
 said communicating device or has been copied
 by said copying device or has been printed by
 said printer;
 said second data processor reducing said roy-
 alty payment amount if said second acknowl- 10
 edgement signal is not received.

7. The method of any one of the claims 1 to 6,
 which further comprises:
 outputting a second authorization message 15
 from said second data processor to said first
 data processor in response to receiving said
 first acknowledgement signal from said first
 data processor;
 said second authorization message giving au- 20
 thorization to communicate said second frac-
 tion of said portion of said document by said
 communicating device or copying device or
 printer. 25
8. The method of any one of claims 1 to 7, which
 further comprises:
 said second data processor counting said ac-
 knowledgement signals from said first data
 processor, to enable resumption of said com- 30
 municating of said document at said second
 fraction if said second acknowledgement signal
 is not received by said second data processor.
9. A computer program which, when executed, 35
 performs a method for managing the printing
 of pages of a structured document on a printer
 device in a network, so as to comply with
 royalty payment requirements of the docu-
 ment, the method comprising the steps of: 40
 inputting into a first data processor in said
 network, a formatted text stream of a struc-
 tured document which includes a royalty pay-
 ment element having a special tag;
 searching said formatted text stream to identify 45
 said royalty payment element and storing a
 royalty payment flag in a memory in said first
 data processor;
 receiving a command from a user to print a
 portion of said document on a printer device 50
 controlled by said first data processor;
 transmitting from said first data processor to a
 second data processor in said network, a re-
 quest for authorization to print said portion of
 said document, in response to said print com- 55
 mand and to said royalty payment flag;
 receiving said request at said second data
 processor and in response thereto, charging

said user a royalty payment amount;
 transmitting from said second data processor
 to said first data processor an authorization
 message for printing said portion of said docu-
 ment;
 receiving said authorization message at said
 first data processor and in response thereto,
 outputting a print control signal from said first
 data processor to said printer to print said
 portion of said document on said printer de-
 vice, or copying device or communicating de-
 vice.

10. A data processing system for managing the
 printing of pages of a structured document on
 a printer device in a network, so as to comply
 with royalty payment requirements of the docu-
 ment, the system comprising:
 input means for inputting into a first data pro-
 cessor in said network, a formatted text stream
 of a structured document which includes a
 royalty payment element having a special tag;
 searching means coupled to said input means,
 for searching said formatted text stream to
 identify said royalty payment element and stor-
 ing a royalty payment flag in a memory in said
 first data processor;
 first receiving means coupled to said memory,
 for receiving a command from a user to print a
 portion of said document on a printer device
 controlled by said first data processor;
 first transmitting means coupled to said mem-
 ory means, for transmitting from said first data
 processor to a second data processor in said
 network, a request for authorization to print
 said portion of said document, in response to
 said print command and to said royalty pay-
 ment flag;
 second receiving means in said second data
 processor, for receiving said request at said
 second data processor and in response there-
 to, charging said user a royalty payment
 amount;
 second transmitting means coupled to said
 second receiving means, for transmitting from
 said second data processor to said first data
 processor an authorization message for print-
 ing said portion of said document;
 authorization receiving means at said first data
 processor, for receiving said authorization
 message at said first data processor and in
 response thereto, outputting a print control sig-
 nal from said first data processor to said print-
 er to print said portion of said document on
 said printer device, or copying device or com-
 munication device.

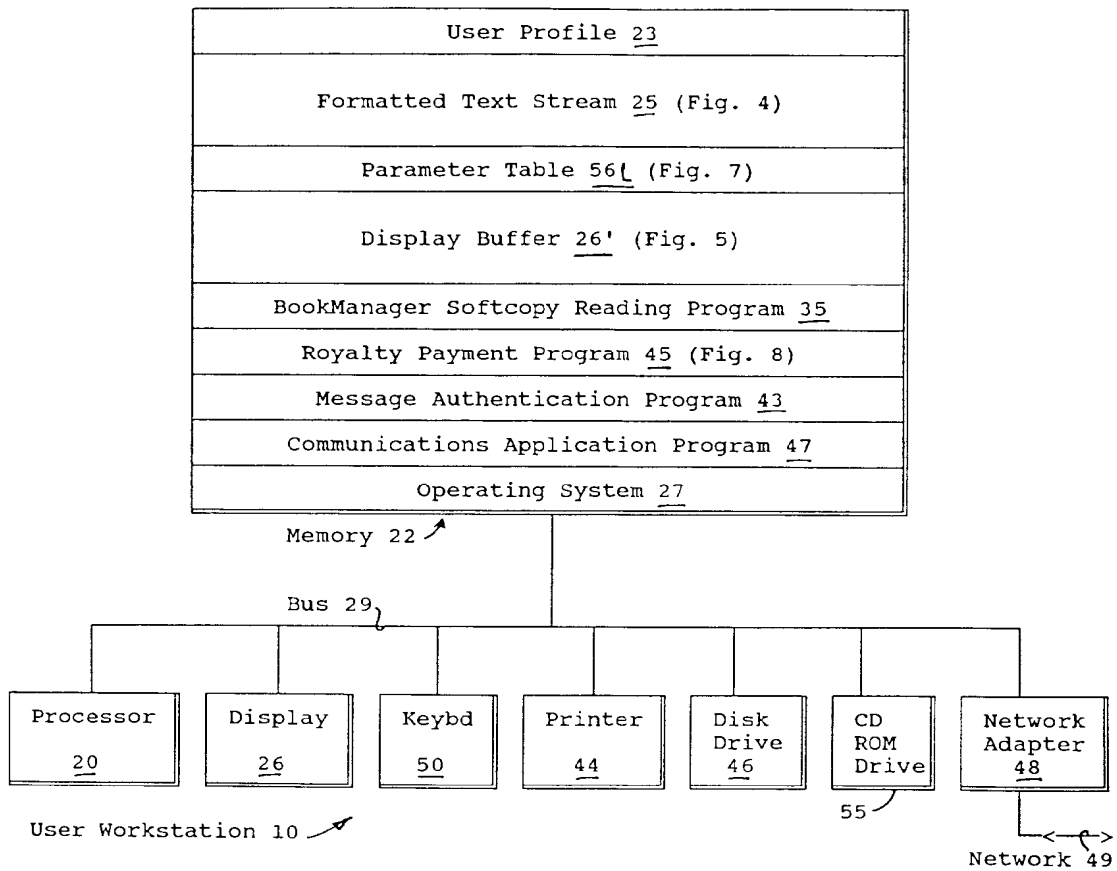


Fig. 1

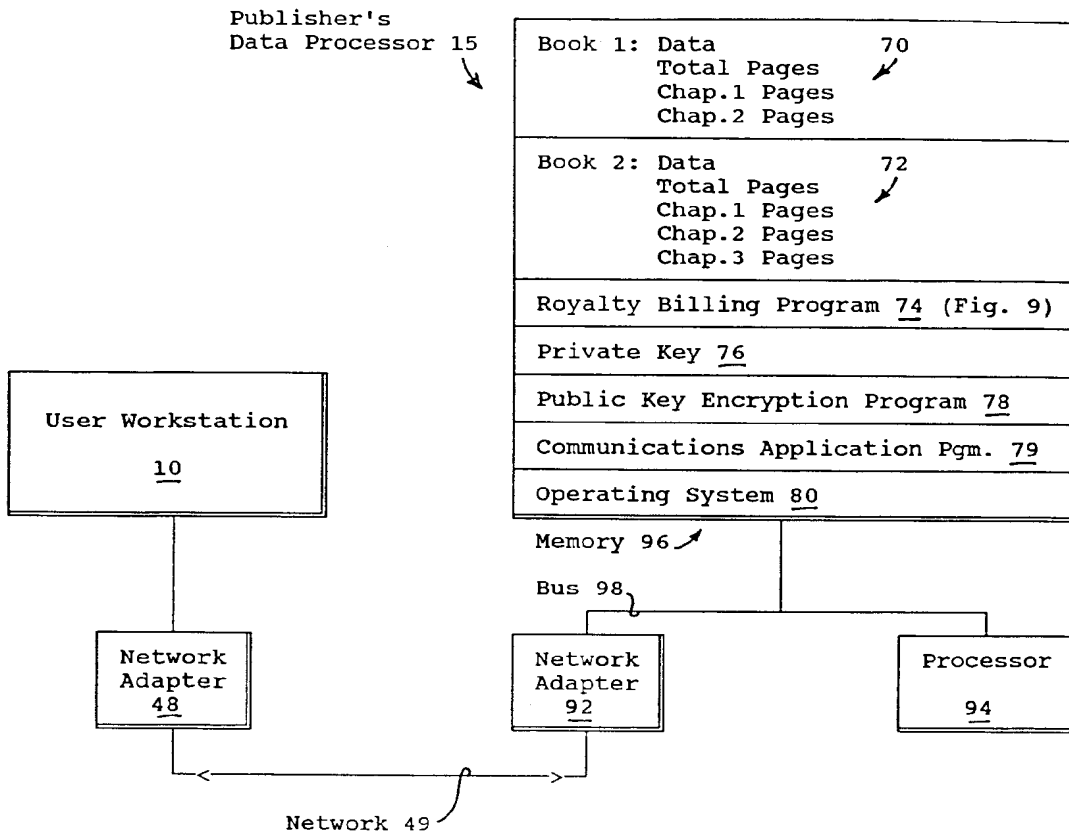


Fig. 2

[cpr](C) Copyright Jefferson & Co. 1776[/cpr]	← copyright 40
[p]We hold these truths to be self-evident, that	] ← paragraph 28
all men are created equal, that they are endowed by	
their Creator with certain unalienable Rights, that	
among these are[/p]	
[list]	
[li]Life, [/li]	← 32
[li]Liberty and [/li]	← 34
[li]the pursuit of Happiness. [/li]	← 36
[/list]	] list 30
[p]That to secure these rights, Governments are	
instituted among Men, deriving their just powers	] ← paragraph 38
from the consent of the governed. [/p]	
[royalty] Book Reproduction Fee [/royalty]	← royalty 306
[amount] \$20.00 [/amount]	← amount 308
	↘ 25

Figure 3A. Example of Control Element Tags and Associated Text

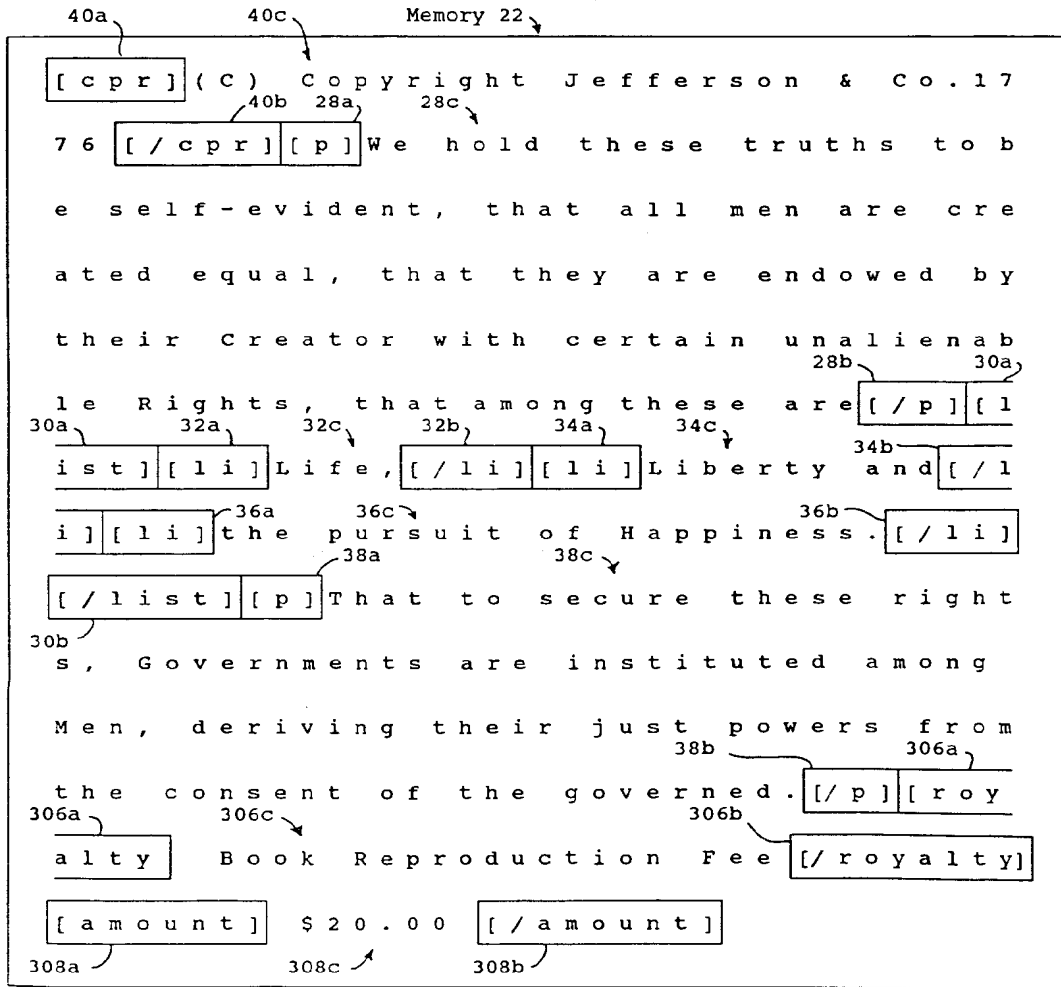


Figure 3B - Memory Organization of Control Element Tags and Associated Text

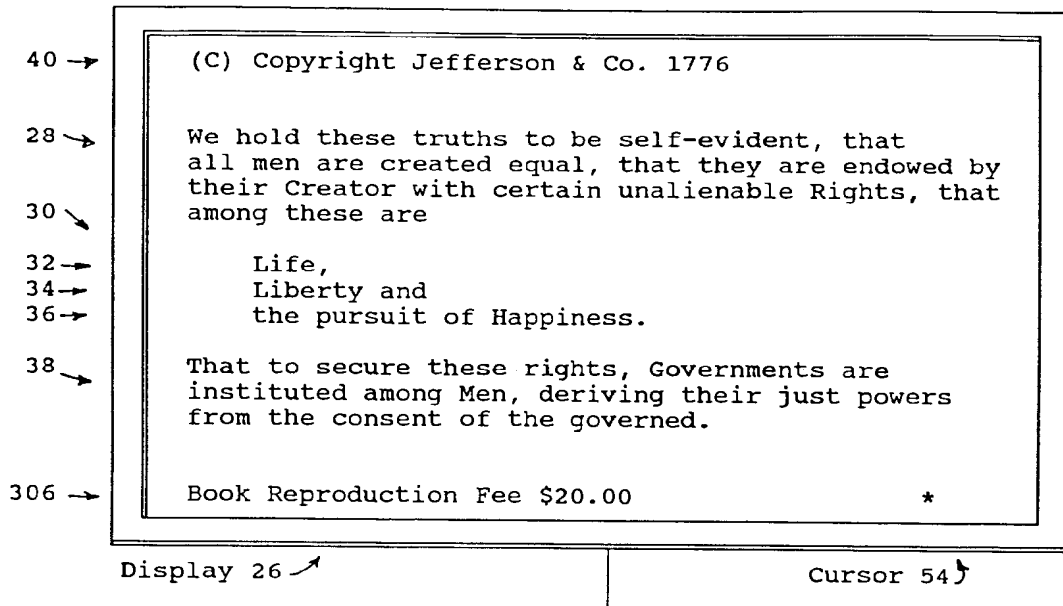


Fig. 3C

Formatted Text Stream 25

coordinates 156

bk h1 h2 h3 p el

300	[bk] Book Title [/bk]	1	0	0	0	0	1
302	[ed] Second Edition [/ed]	1	0	0	0	1	1
304	[cpr] (C) ABC Co 1990 [/cpr]	1	0	0	0	2	1
306	[royalty] Book Reproduction Fee [/royalty]	1	0	0	0	3	1
308	[amount] \$20.00 [/amount]	1	0	0	0	3	2
310	[phone] 1-800-123-1234 [/phone]	1	0	0	0	3	3
312	[public key] 13A723F9...6 [/public key]	1	0	0	0	3	4
314	[validation] The Book Repro Fee Is Paid [/validation]	1	0	0	0	3	5
316	[h1] First Chapter Heading [/h1]	1	1	0	0	0	1
318	[royalty] Chapter Reproduction Fee [/royalty]	1	1	0	0	1	1
320	[amount] \$ 1.00 [/amount]	1	1	0	0	1	2
322	[validation] First Chapter Fee Paid [/validation]	1	1	0	0	1	3
324	[p] Paragraph of text [/p]	1	1	0	0	2	1
326	[h2] First topic heading [/h2]	1	1	1	0	0	1
328	[p] Paragraph of text [/p]	1	1	1	0	1	1
330	[p] Paragraph of text [/p]	1	1	1	0	2	1
332	[h2] Second topic heading [/h2]	1	1	2	0	0	1
334	[p] Paragraph of text [/p]	1	1	2	0	1	1
336	[h3] First subtopic heading [/h3]	1	1	2	1	0	1
338	[p] Paragraph of text [/p]	1	1	2	1	1	1
340	[p] Paragraph of text [/p]	1	1	2	1	2	1
342	[h1] Second Chapter Heading [/h1]	1	2	0	0	0	1
344	[royalty] Chapter Reproduction Fee [/royalty]	1	2	0	0	1	1
346	[amount] \$ 2.00 [/amount]	1	2	0	0	1	2
348	[validation] Second Chapter Fee Paid [/validation]	1	2	0	0	1	3
350	[p] Paragraph of text [/p]	1	2	0	0	2	1

Memory 22

Figure 4 - Memory Image of Formatted Text and Element Coordinates

300 → Book Title
 302 → Second Edition
 304 → (C) ABC Co 1990
 306 → Book Reproduction Fee
 308 → \$20.00
 310 → 1-800-123-1234
 :

 :
 316 → First Chapter Heading
 318 → Chapter Reproduction Fee
 320 → \$ 1.00
 324 → Paragraph of text
 326 → First topic heading
 328 → Paragraph of text
 330 → Paragraph of text
 332 → Second topic heading
 334 → Paragraph of text
 336 → First subtopic heading
 338 → Paragraph of text
 340 → Paragraph of text
 :

 :
 342 → Second Chapter Heading
 344 → Chapter Reproduction Fee
 346 → \$ 2.00
 350 → Paragraph of text

Display 26 ↗

Figure 5 - Display of Text from Fig. 4

Initially Unloaded Parameter Table 56

	360 Special Tags	362 Text String Loaded from Elements with Special Tags	156 Element Coordinates bk h1 h2 h3 p el	364 Dis- play Text	366 Book Royalty Flag	368 Chapter Royalty Flag
300I	bk			yes		
302I	ed			yes		
304I	cpr			yes		
306I	royalty			yes		
308I	amount			yes		
310I	phone			yes		
312I	public key			no		
314I	validation			no		

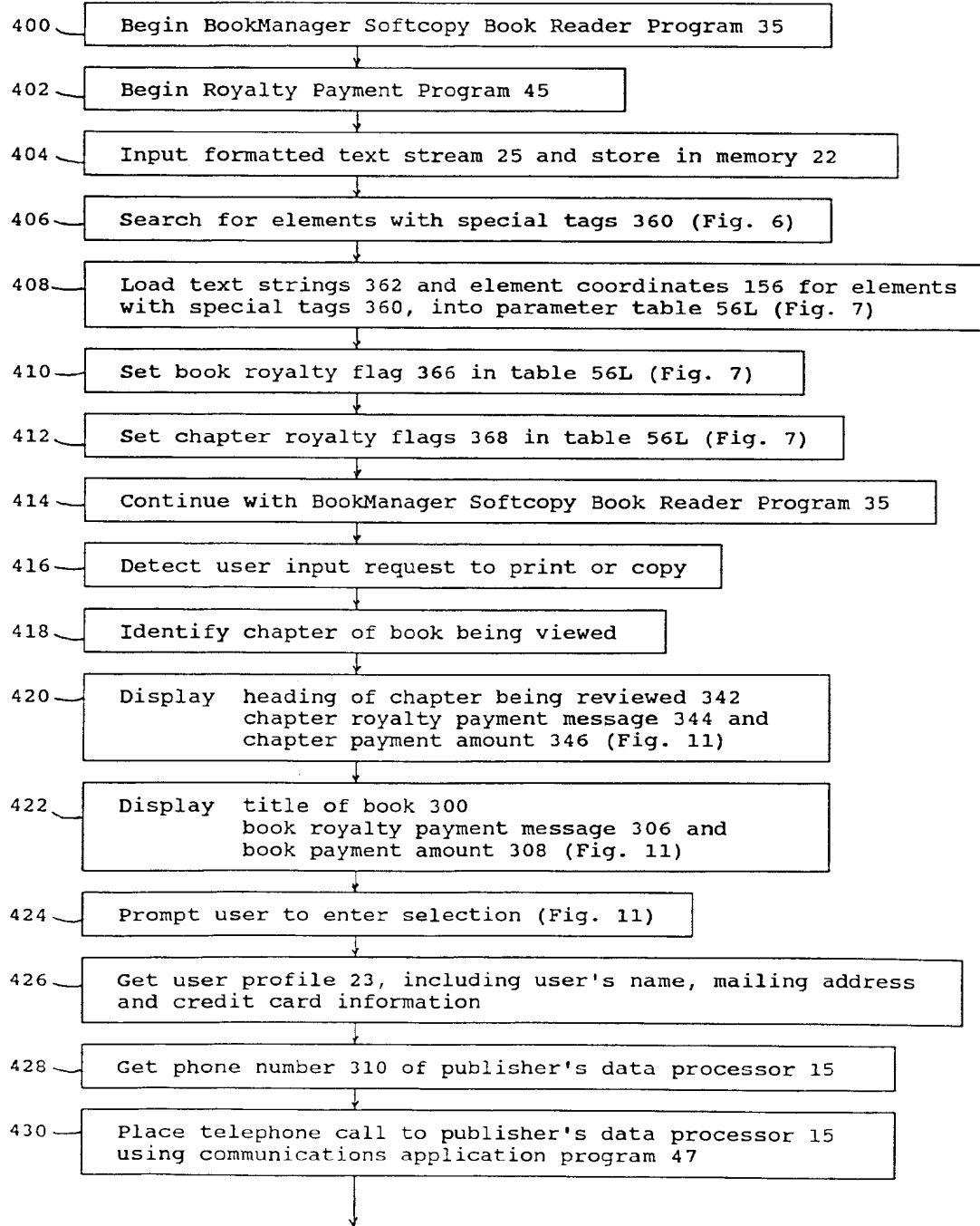
Fig. 6

Loaded Parameter Table 56L

	360 ↙ Special Tags	362 ↙ Text String Loaded from Elements with Special Tags	156 ↙ Element Coordinates bk h1 h2 h3 p el	364 ↙ Dis- play Text	366 ↙ Book Royalty Flag	368 ↙ Chapter Royalty Flag
300L	bk	Book Title	1 0 0 0 0 1	yes		
302L	ed	Second Edition	1 0 0 0 1 1	yes		
304L	cpr	(C) ABC Co. 1990	1 0 0 0 2 1	yes		
306L	royalty	Book Repro...Fee	1 0 0 0 3 1	yes	x	
308L	amount	\$20.00	1 0 0 0 3 2	yes		
310L	phone	1-800-123-1234	1 0 0 0 3 3	yes		
312L	public key	13A723F9...6	1 0 0 0 3 4	no		
314L	validation	The Book ... Paid	1 0 0 0 3 5	no		
318L	royalty	Chapt...Repro Fee	1 1 0 0 1 1	yes		x
320L	amount	\$ 1.00	1 1 0 0 1 2	yes		
322L	validation	First Chapt...Paid	1 1 0 0 1 3	no		
344L	royalty	Chapt...Repro Fee	1 2 0 0 1 1	yes		x
346L	amount	\$ 2.00	1 2 0 0 1 2	yes		
348L	validation	Second Chapt..Paid	1 2 0 0 1 3	no		

Fig. 7

Fig. 8



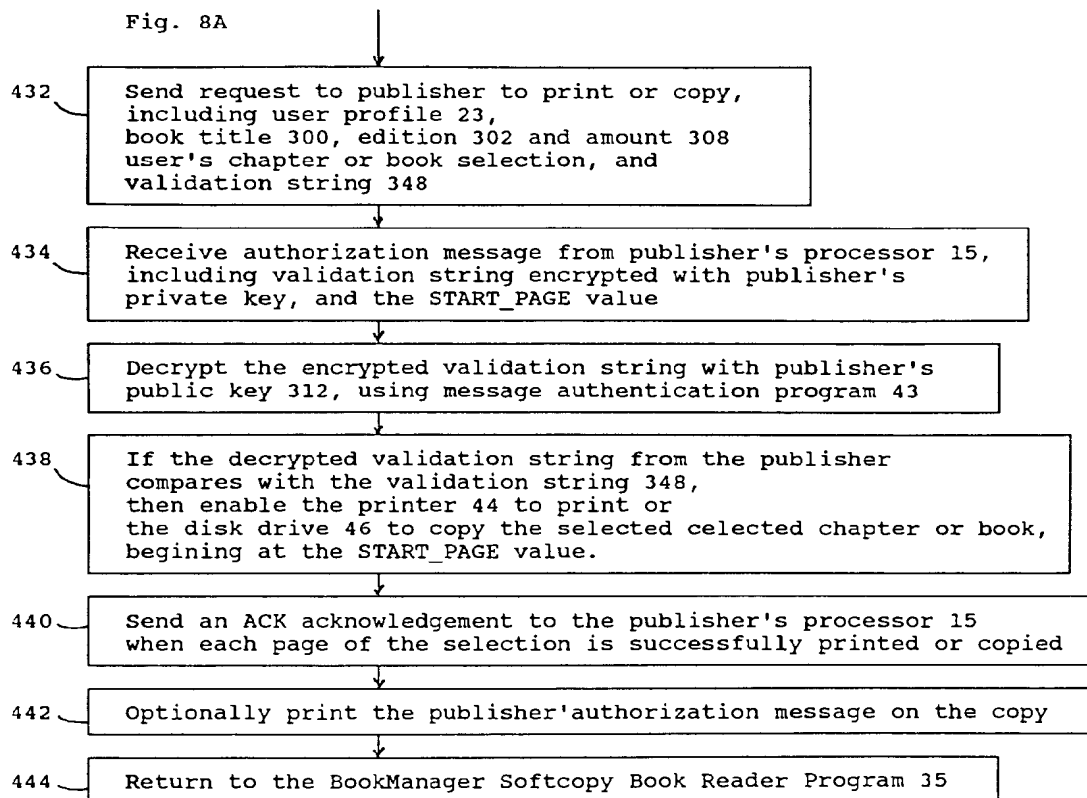


Fig. 9

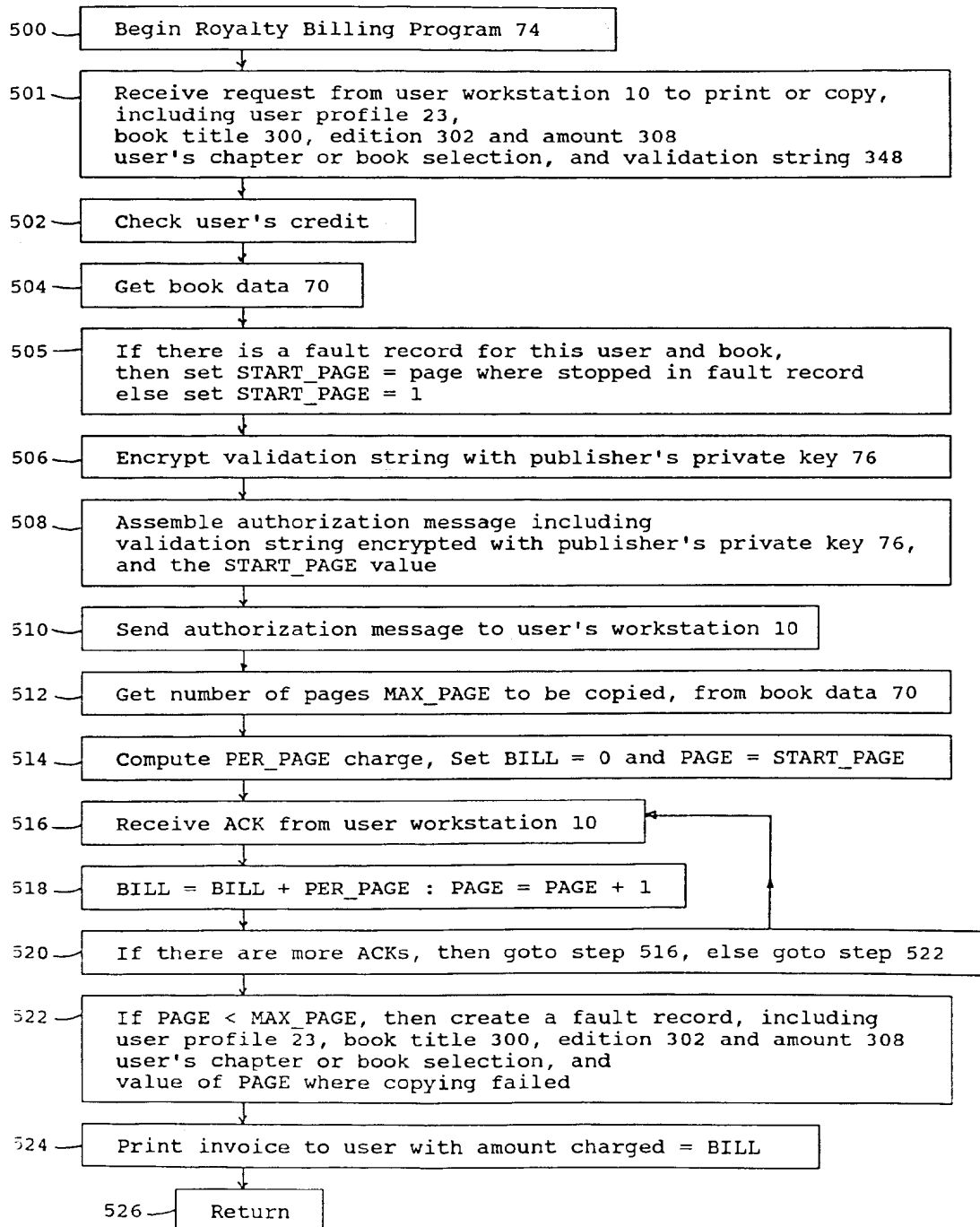
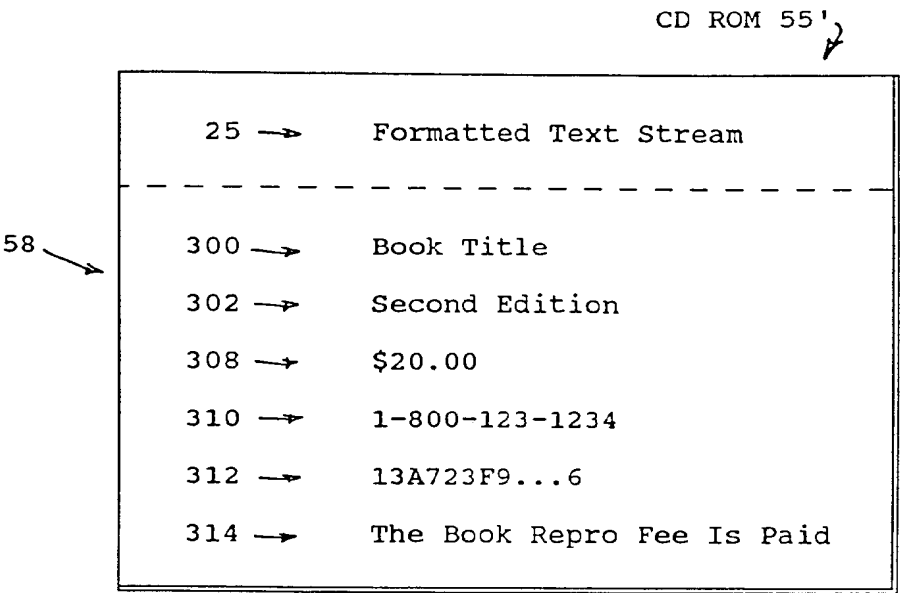


Fig. 10



Reproduction Fees

For Current Chapter Being Viewed

342 → Second Chapter Heading Type "X" in box

344 → Chapter Reproduction Fee ☐

346 → \$ 2.00

Reproduction Fees

For The Entire Book Being Viewed

300 → Book Title Type "X" in box

302 → Second Edition ☐

306 → Book Reproduction Fee

308 → \$20.00

Enter Your Selection and Then Call

310 → 1-800-123-1234

The amount you select will be billed
to the credit card number in your profile.

Display 26 ↗

Figure 11 - Display of Prompt to User



European Patent
Office

EUROPEAN SEARCH REPORT

Application Number

EP 93 10 5502

DOCUMENTS CONSIDERED TO BE RELEVANT			
Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int. Cl.5)
D,Y D,A	EP-A-0 464 306 (IBM) * the whole document *	1-3,9,10	G06F1/00
Y	US-A-4 685 055 (THOMAS) * figure 1 *	1-3,9,10	
A	* column 1, line 41 - line 55 * * column 4, line 9 - column 6, line 28 * -----	4,5	
			TECHNICAL FIELDS SEARCHED (Int. Cl.5)
			G06F G07F
The present search report has been drawn up for all claims			
Place of search THE HAGUE		Date of completion of the search 20 JULY 1993	Examiner WEISS P.
CATEGORY OF CITED DOCUMENTS X : particularly relevant if taken alone Y : particularly relevant if combined with another document of the same category A : technological background O : non-written disclosure P : intermediate document T : theory or principle underlying the invention E : earlier patent document, but published on, or after the filing date D : document cited in the application L : document cited for other reasons & : member of the same patent family, corresponding document			

EPO FORM 1503 (01.82 (P0401))

Electronic Patent Application Fee Transmittal				
Application Number:		13585408		
Filing Date:		14-Aug-2012		
Title of Invention:		SYSTEM AND METHOD FOR DISTRIBUTING DIGITAL CONTENT TO BE RENDERED IN ACCORDANCE WITH USAGE RIGHTS INFORMATION		
First Named Inventor/Applicant Name:		Mark J. Stefik		
Filer:		Stephen M. Hertzler		
Attorney Docket Number:		10-510-US-C73		
Filed as Large Entity				
Utility under 35 USC 111(a) Filing Fees				
Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Miscellaneous:				
Submission- Information Disclosure Stmt	1806	1	180	180
Total in USD (\$)				180

Electronic Acknowledgement Receipt

EFS ID:	15054874
Application Number:	13585408
International Application Number:	
Confirmation Number:	4941
Title of Invention:	SYSTEM AND METHOD FOR DISTRIBUTING DIGITAL CONTENT TO BE RENDERED IN ACCORDANCE WITH USAGE RIGHTS INFORMATION
First Named Inventor/Applicant Name:	Mark J. Stefik
Customer Number:	98804
Filer:	Stephen M. Hertzler
Filer Authorized By:	
Attorney Docket Number:	10-510-US-C73
Receipt Date:	26-FEB-2013
Filing Date:	14-AUG-2012
Time Stamp:	21:42:24
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Credit Card
Payment was successfully received in RAM	\$ 180
RAM confirmation Number	9221
Deposit Account	501529
Authorized User	HERTZLER, STEPHEN M.

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.19 (Document supply fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.21 (Miscellaneous fees and charges)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Information Disclosure Statement (IDS) Form (SB08)	10-510-US-C73_-_2013-02-26_-_Information_Disclosure_Statement.pdf	613281 eee3f8933a827ef86671b806045e0844284412a0	no	6
Warnings:					
Information:					
2	Foreign Reference	10-510-US-C73_-_2013-02-26_-_EP0268139A.pdf	2712001 b677e06893aefcca3714cb04dc7f18d8ed0bb0957	no	43
Warnings:					
Information:					
3	Foreign Reference	10-510-US-C73_-_2013-02-26_-_EP0464306A2.pdf	1647131 43050ded7e262f0550742d6c8e79403ad8e2ed33	no	27
Warnings:					
Information:					
4	Foreign Reference	10-510-US-C73_-_2013-02-26_-_EP0567800A1.pdf	1723309 6ea1cb659b49a20d182ab59160723c16042c1c95	no	29
Warnings:					
Information:					
5	Fee Worksheet (SB06)	fee-info.pdf	30631 050fe36c7b0def0d8353bf3ec6595d7a73706a5c	no	2
Warnings:					
Information:					
Total Files Size (in bytes):			6726353		

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.