(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
19 December 2002 (19.12.2002)

PCT

(10) International Publication Number
WO 02/101577 A1

(51) International Patent Classification[7]: G06F 17/00

(21) International Application Number: PCT/US02/17851

(22) International Filing Date: 6 June 2002 (06.06.2002)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/296,114 7 June 2001 (07.06.2001) US

(71) Applicant: CONTENTGUARD HOLDINGS, INC. [US/US]; 103 Foulk Road, Suite 200-M, Wilmington, DE 19803 (US).

(72) Inventor: LAO, Guillermo; 5531 Lorna Street, Torrance, CA 90503 (US).

(74) Agent: KAUFMAN, Marc, S.; Nixon Peabody LLP, 8180 Greensboro Drive, Suite 800, McLean, VA 22102 (US).

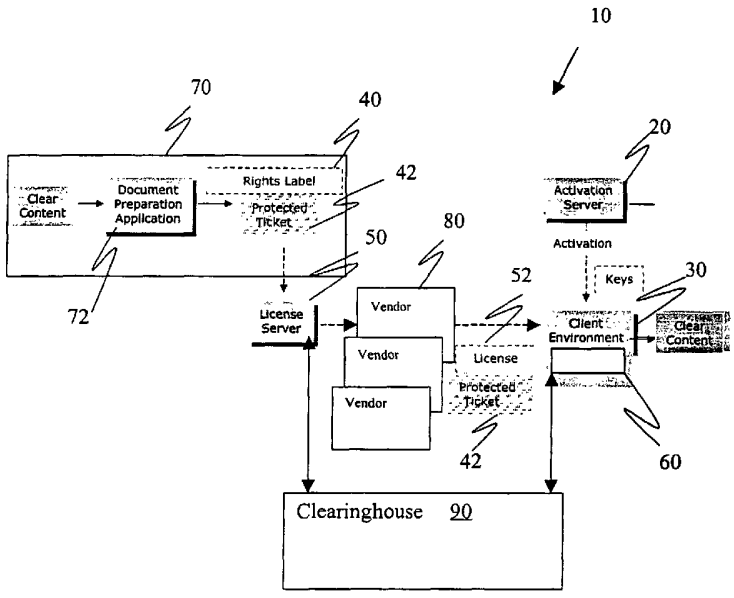
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZM, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: METHOD AND SYSTEM FOR SUBSCRIPTION DIGITAL RIGHTS MANAGEMENT



(57) Abstract: A system and method (10) for managing use of items having usage rights associated therewith. The system includes an activation device (20) adapted to issue a software package having a public and private key pair, the public key being associated with a user, a license device (50) adapted to issue a license (52), a usage device adapted to receive the software package, receive the license and allow the user to access the item in accordance with the license, and a subscription managing device adapted to maintain a subscription list including the public key associated with the user. Licenses is issued by the license device (50) upon verifying presence of the public key in the subscription list corresponding to requested content.

WO 02/101577 A1

METHOD AND SYSTEM FOR SUBSCRIPTION DIGITAL RIGHTS MANAGEMENT

BACKGROUND OF THE INVENTION

Field of the Invention

[0001] The present invention is directed to a subscription digital rights management system and a method thereof. In particular, the present invention is directed to such a system and method that facilitates subscription to plural protected items, such as digital content.

Description of Related Art

[0002] One of the most important issues impeding the widespread distribution of digital works (i.e. documents or other content in forms readable by computers), via electronic means, and the Internet in particular, is the current lack of ability to enforce the intellectual property rights of content owners during the distribution and use of digital works. Efforts to resolve this problem have been termed "Intellectual Property Rights Management" ("IPRM"), "Digital Property Rights Management" ("DPRM"), "Intellectual Property Management" ("IPM"), "Rights Management" ("RM"), and "Electronic Copyright Management" ("ECM"), collectively referred to as "Digital Rights Management (DRM)" herein. There are a number of issues to be considered in effecting a DRM System. For example, authentication, authorization, accounting, payment and financial clearing, rights specification, rights verification, rights enforcement, and document protection issues should be addressed. U.S. patents 5,530,235, 5,634,012, 5,715,403, 5,638,443, and 5,629,980, the disclosures of which are incorporated herein by reference disclose DRM systems addressing these issues.

[0003] In the world of printed documents and other physical content, a work created by an author is usually provided to a publisher, which formats and prints numerous copies of the work. The copies are then sent by a distributor to bookstores or other retail outlets, from which the copies are purchased by end users. While the low quality of copying and the high cost of distributing printed material have served as deterrents to unauthorized copying of most printed documents, it is far too easy to copy, modify, and redistribute unprotected digital works with high quality. Accordingly, mechanisms of protecting digital works are necessary to retain rights of the owner of the work.

[0004] Unfortunately, it has been widely recognized that it is difficult to prevent, or even deter, people from making unauthorized copies of electronic works within current general-purpose computing and communications systems such as personal computers, workstations, and other devices connected over communications networks, such as local area networks (LANs), intranets, and the Internet. Many attempts to provide hardware-based solutions to prevent unauthorized copying have proven to be unsuccessful. The proliferation of high band-width "broadband" communications technologies and the development of what is presently known as the "National Information Infrastructure" (NII) will render it even more convenient to distribute large documents electronically, including video files such as full length motion pictures, and thus will remove any remaining deterrents to unauthorized copying and distribution of digital works. Accordingly, DRM technologies are becoming a high priority.

[0005] Two basic DRM schemes have been employed, secure containers and trusted systems. A "secure container" (or simply an encrypted document) offers a way to keep document contents encrypted until a set of authorization conditions are met and some copyright terms are honored (e.g., payment for use). After the various conditions and terms are verified with the document

provider, the document is released to the user in clear form. Commercial products such as CRYPTOLOPES™ and DIGIBOXES™ fall into this category. Clearly, the secure container approach provides a solution to protecting the document during delivery over insecure channels, but does not provide any mechanism to prevent legitimate users from obtaining the clear document and then using and redistributing it in violation of content owners' intellectual property.

[0006] In the "trusted system" approach, the entire system is responsible for preventing unauthorized use and distribution of the document. Building a trusted system usually entails introducing new hardware such as a secure processor, secure storage and secure rendering devices. This also requires that all software applications that run on trusted systems be certified to be trusted. While building tamper-proof trusted systems is a real challenge to existing technologies, current market trends suggest that open and untrusted systems, such as PC's and workstations using browsers to access the Web, will be the dominant systems used to access digital works. In this sense, existing computing environments such as PC' s and workstations equipped with popular operating systems (e.g., Windows™, Linux™, and UNIX) and rendering applications, such as browsers, are not trusted systems and cannot be made trusted without significantly altering their architectures. Of course, alteration of the architecture defeats a primary purpose of the Web, i.e. flexibility and compatibility.

[0007] U.S. patent 5,634,012, the disclosure of which is incorporated herein by reference, discloses a system for controlling the distribution of digital documents. Each rendering device has a repository associated therewith. A predetermined set of usage transaction steps define a protocol used by the repositories for enforcing usage rights associated with a document. Usage rights persist with the document content. The usage rights can permit various manners of use such as, viewing only, use once,

distribution, and the like. Usage rights can be contingent on payment or other conditions.

[0008] Conventional DRM systems typically provide access to protected content after a transaction in which an end user obtains a license allowing access to the protected content. Thus, conventional DRM systems utilize a "per-transaction" model where each access to the protected content requires a separate transaction with a separate license. In this regard, conventional DRM systems can become very cumbersome when a user expects to access a large number of items of protected content since a transaction must be made for each item accessed.

SUMMARY OF THE INVENTION

[0009] A first aspect of the invention is a DRM system for distributing items having usage rights associated therewith in accordance with one embodiment of the present invention comprising an activation device adapted to issue a software package that enforces usage rights to control use of the items, the software package having a public and private key pair, the public key being associated with a user, a license device adapted to issue a license having usage rights associated with at least one item, a usage device adapted to receive the software package, receive the license associated with the at least one item, and allow the user to access the at least one item in accordance with the license, and a subscription managing device adapted to maintain a subscription list including the public key associated with the user, where the license is issued by the license device upon verifying presence of the public key in the subscription list.

[0010] A second aspect of the present invention is a method for distributing items having usage rights associated therewith, the method comprising the steps of providing a software package to at least one user, the software package enforcing usage rights to control use of the items and having a

private key and a public key associated with the at least one user, storing the public key associated with the at least one user in a subscription list, receiving a request from the at least one user to access the at least one item, verifying that the at least one user requesting access to the at least one item is listed in the subscription list, and issuing a license that grants usage rights to the at least one user to use the at least one item.

BRIEF DESCRIPTION OF THE DRAWINGS

[0011] Fig. 1 is a schematic illustration of a DRM system adapted to a per-transaction model;

[0012] Fig. 2 is a schematic illustration of a rights label of the preferred embodiment;

[0013] Fig. 3 is a schematic illustration of a license of the preferred embodiment;

[0014] Fig. 4 is a schematic illustration of a DRM system in accordance with an embodiment of the present invention that provides subscription access to protected content; and

[0015] Fig. 5 is a flow chart of a method of the preferred embodiment.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

[0016] A DRM System can be utilized to specify and enforce usage rights for items, such as digital content, services, or goods property. Fig. 1 illustrates DRM system 10 that can be used to distribute digital content. DRM System 10 includes a user activation component, in the form of activation server 20, that issues public and private key pairs to content users in a protected fashion, as is well known.

[0017] Typically, when a user uses DRM System 10 for the first time, the user is activated. During an activation process, some information is exchanged between activation server 20 and a device associated with the user, such as client environment 30, and client component 60 is downloaded and installed in client environment 30. Client component 60 preferably is tamper resistant and contains the set of public and private keys issued by activation server 20 as well as other components such as any necessary engine for parsing or rendering protected items such as protected content 42.

[0018] Rights label 40 is associated with protected content 42 and specifies usage rights that are available to an end-user when corresponding conditions are satisfied. Protected content 42 specifies a specific item as described below. License server 50 manages the encryption keys and issues licenses 52 for exercise of rights in the manner set forth below. Licenses 52 embody the actual granting of rights to an end user. For example, license 52 may permit a user to view protected content 42 for a fee of five dollars. Client component 60 interprets and enforces the rights that have been specified in license 52.

[0019] Fig. 2 illustrates rights label 40 in accordance with the preferred embodiment. Rights label 40 includes plural rights offers 44. Each rights offer 44 includes usage rights 44a, conditions 44b, and content specification 44c. Content specification 44c can include any mechanism for referencing, calling, locating, or otherwise specifying content 42 associated with rights offer 44.

[0020] Fig. 3 illustrates license 52 in accordance with the preferred embodiment. License 52 includes a unique license ID 52a, grant 52b (including usage rights, a principal, conditions, and state variables) and a content specification designating content 42 associated with license 52. License 52 also includes digital signature 52c including any cryptographic keys or the like for unlocking item ticket 42.

[0021] Usage rights specify manners of use. For example, a manner of use can include the ability to use an item in a specified way such as to print, copy, view, or the like. Rights can also be bundled. Further, usage rights can specify transfer rights, such as distribution rights. In some cases conditions must be satisfied in order to exercise the manner of use in a specified usage right. For, example a condition may be the payment of a fee, submission of personal data, or any other requirement desired before permitting exercise of a manner of use. Conditions can also be "access conditions" for example, access conditions can apply to a particular group of users, say students in a university, or members of a book club. In other words, the condition is that the user is a particular person or member of a particular group. Rights and conditions can exist as separate entities or can be combined.

[0022] State variables track potentially dynamic states conditions. State variables are variables having values that represent status of an item, usage rights, license or other dynamic conditions. State variables can be tracked, by clearinghouse 90 or another device, based on identification mechanisms in license 52 and ticket 42. Further, the value of state variables can be used in a condition. For example, a usage right can be the right to redeem item ticket 42 for specified goods and a condition can be that the usage right can be exercised three times. Each time the usage right is exercised, the value of the state variable is incremented. In this example, when the value of the state variable is three, the condition is not longer satisfied and ticket 42 cannot be redeemed. Another example of a state variable is time. A condition of license 52 may require that item ticket 42 is redeemed within thirty days. A state variable can be used to track the expiration of thirty days. Further, the state of a usage right can be tracked as a collection of state variables. The collection of the change is the state of a usage right represents the usage history of that right.

[0023] Protected content 42 can be prepared with document preparation application 72 installed on computer 70 associated with the distributor of content, a content service provider, or any other party. Preparation of protected content 42 consists of specifying the rights and conditions under which protected content 42 can be used by associating rights label 40 with protected content 42 and protecting protected content 42 with some crypto algorithm or other mechanism for preventing processing or rendering of protected content 42. A rights language such as XrML™ can be used to specify the rights and conditions in rights label 40. However, the rights and conditions can be specified in any manner. Accordingly, the process of specifying rights refers to any process for associating rights with protected content 42. Rights label 40 associated with protected content 42 and the encryption key used to encrypt protected content 42 can be transmitted to license server 50. Protected content 42 can be a text file an audio file, a video file, a digital multimedia file, or any other digital content.

[0024] A typical workflow for DRM System 10 is described below. A user operating within client environment 30 is activated for receiving protected content 42 by activation server 20. This results in a public-private key pair (and possibly some user/machine specific information) being downloaded to client environment 30 in the form of client software component 60 in a known manner. This activation process can be accomplished at any time prior to the issuing of a license.

[0025] When a user wishes to obtain a specific protected content 42, the user makes a request for the protected content 42. For example, a user might browse a Web site running on Web server of vendor 80, using a browser installed in client environment 30, and request an item corresponding to protected content 42. The user can examine rights offers 44 in rights label 40 associated with protected content 42 and select the desired usage rights. During this process, the user may go through a series of steps possibly to

satisfy conditions of the usage rights including a fee transaction or other transactions (such as collection of information). When the appropriate conditions and other prerequisites, such as the collection of a fee and verification that the user has been activated, are satisfied, vendor 80 contacts license server 50 through a secure communications channel, such as a channel using a Secure Sockets Layer (SSL). License server 50 then generates license 52 for protected content 42 and vendor 80 causes both protected content 42 and license 52 to be downloaded. License 52 includes the usage rights selected and can be downloaded from license server 50 or an associated device. Protected content 42 can be downloaded from computer 70 associated with a vendor, distributor, or other party.

[0026] Client component 60 in client environment 30 will then proceed to interpret license 52 and allow the use of protected content 42 based on the rights and conditions specified in license 52. The interpretation and enforcement of usage rights and related systems and techniques are well known. The steps above may take place sequentially or approximately simultaneously or in various sequential order.

[0027] DRM System 10 addresses security aspects of protected contents 42. In particular, DRM System 10 may authenticate license 52 that has been issued by license server 50. One way to accomplish such authentication is for application 60 to determine if licenses 52 can be trusted. In other words, application 60 has the capability to verify and validate the cryptographic signature, or other identifying characteristic of license 52. Of course, the example above is merely one way to effect a DRM System. For example, license 52 and protected content 42 can be distributed from different entities. Clearinghouse 90 can be used to process payment transactions and verify payment prior to issuing a license.

[0028] DRM systems such as the one described above provide access to protected items, such as protected content, after activation in which an end

user obtains software and a license to access the protected content. A license is issued, and thus an exchange of keys or other identifying mechanisms must be accomplished, for each item of protected content. This per-transaction model can become cumbersome when a user expects to access and use a large number of items of protected content since a license must be generated for each protected content. In contrast, the DRM system and method in accordance with the preferred embodiment is implemented using a subscription model to provide automated user access to a collection of protected content without necessitating activation of a license for each protected content accessed.

[0029] It should be initially noted that the term "subscription" is used in a generic sense and includes any item, such as protected content, that a user is allowed to access. The subscription could involve delivery of an electronic document, or delivery of a means to obtain a hard copy document or other goods or services. For example, subscriptions may be periodicals, monthly bills or banks statements or access to a streaming media service. Subscription may also be subscriptions to tickets or other vouchers which are used to access or obtain other content, resources, physical goods or service.

[0030] In addition, it should be understood that whereas terms "server" and "client" are used below to describe the devices for implementing the present invention in the embodiment discussed herein, these terms should be broadly understood to mean any appropriate device for executing the function described. For instance, a personal computer, laptop, PDA or other hand held device, PDAs, or any other general purpose programmable computer, or combination of such devices, such as a network of computers may be used.

[0031] DRM system 100 in accordance with an embodiment of present invention is illustrated in Fig. 4. DRM system 100 that allows subscription based use of items, such as protected content 108. Because items of protected content 108 are encrypted or otherwise protected, they cannot be

used by end users 114 without licenses 116 and software package 103 as a security component. DRM system 100 includes an activation device such as activation server 102 that is adapted to issue software package 103 to a usage device such as client 106 to allow one or more end users 114 to use a plurality of items of protected content 108. Activation server 102 of the DRM system 100 provides a public and private key pair to client 106, each of the end users 114 having at least a public key associated therewith.

[0032] DRM system 100 also includes a license device, such as license server 110, that is adapted to issue licenses 116 having usage rights which are associated with plurality of protected content 108. These licenses 116 define the end user's rights regarding a particular item of protected content 108. Requests for licenses 116 from license server 110 are made by distribution point 128 based on requests of end users 114 via client 106. A separate client device can be associate with each end user 114 or end users 114 can use a common client device. License 116 allows authorized end users 114 to access and use protected content 103. When license server 110 issues requested licenses 116', distribution point 128 pre-packages licenses 116' with the appropriate protected content 108 so that licenses 116' are matched to protected content 108 as shown in Fig. 4. When pre-packaged, licenses 116' can be a part of protected content 108 in the manner shown in Fig. 4. However, licenses 116' may also be a separate file or other component with a mechanism to associate the license to the appropriate protected content. For example, a link, a reference, a call or other association mechanism can be used. Client 106 receives software 103 package from activation server 102, receives protected content 108 with license 116' associated thereto in a pre-packaged form from distribution point 128, and allows one or more end users 114 to access protected content 108 for which the end user is authorized.

[0033] In the subscription based implementation, DRM system 100 allows end users 114 to access a plurality of protected content 108 without necessitating a separate activation for each item of protected content. In particular, DRM system 100 is adapted to be operated in subscription based manner and to provide subscribing end users 114 access to a plurality of items of protected content 108 without requiring further activations by activation server 102 and the corresponding delay and overhead.

[0034] DRM system 100 of the present embodiment is provided with a subscription managing device such as subscription list manager 120 that is adapted to recognize the identity of each end user 114 by maintaining a subscription list of public keys associated to each of subscribing end user 114. Subscription list manager 120 of the illustrated embodiment is also provided with database 122 for storing such identity information and public key information associated with end users 114. By having a subscription list and comparing the utilized public key with the public keys in the subscription list, DRM system 100 knows the identity of the subscribing end users 114 seeking to access and use specific protected content. When distribution point 128 requests a license on behalf of a particular end user who is a subscriber, the public key associated with the particular end user is extracted from the stored list in database 122 by subscription list manager 120 and the public key is used by license server 110 to issue the requisite license.

[0035] In the illustrated embodiment of Fig. 4, DRM system 100 would be used in the following manner to affect the method illustrated in Fig. 5. First, end users 114 utilize client environment 106 to be activated by server 102 in the manner described above (step 502). End users 114 join a subscription that is offered through a distribution point 128 which can be implemented as an application through a web site, an online store, or in another appropriate manner in step 504. During the process of joining a subscription, a series of steps may be provided to create an account or arrange payment of a fee in

any appropriate manner. The details of the creation of the account or payment of the fee can be accomplished using known user interfaces and known APIs, or the likes and thus, is not discussed in further detail herein.

[0036] After receiving a request for content in step 506, distribution point 128 retrieves the public keys that are associated with each end user 114, requesting protected content 108, the public keys being obtained during the activation process from activation server 102. The public keys identify end users and are stored in database 122 in correspondence with the associated end user and other associated data. When protected content 108 is to be distributed to subscribing end users 114, for instance through e-mail, distribution point 128 makes requests to license server 110 to issue the appropriate licenses. Requests for licenses may include a list of end users, their respective public encryption keys, and the protected content ID for which the licenses are to be issued. Of course, the request could also be for licensing a single end user or multiple protected content as well. The request for licenses may be executed using an API or by any other appropriate protocol.

[0037] License server 110 then authenticates the requester such as distribution point 128, checks that the end users are on the appropriate subscription list (step 508), and if so, issues licenses 116 (step 510), and delivers them to distribution point 128 for pre-packaging with protected content 108. The distribution point 128 pre-packages protected content 108 with licenses 116' and delivers them, or otherwise makes them available, to each end user 114 (step 512). Since items of protected content 108 are delivered pre-packaged with an issued license 116, users would not need to go through additional activations/procedures and wait for licenses to issue in order to access and use protected content 108 of the subscription after the initial activation. Subscription lists are maintained by subscription list manger

120 and correlated to the public keys, to verify if the user is entitled to license 116.

[0038] As noted above, it is desirable to pre-package license 116' with content 108 when it is delivered by distribution point 128 to end users 114 in order to provide a more seamless user experience. In the illustrated embodiment of Fig. 4, distribution point 128, which is merely schematically shown, may be a computer application or a storefront such as a web based, on-line store or vendor. Alternatively, distribution point 128 may be a computer application that is integrated with a mail server, license server 110, or subscription list manager 120 that maintains a subscription list. In such embodiments, maintenance of the subscription list could be as simple as storing the public keys in database 122, within a mail server directory, or a link to another storage location where public keys can be stored and managed. In an enterprise such as a group, company or entity, distribution lists may be adapted to be subscription lists. Any number of subscription lists can be managed.

[0039] In the above described manner, DRM system 100 facilitates end users access to large number of items of protected content without the need for repeated activations for each license. It should also be noted that the above discussed sequence of steps illustrate only one example workflow of how a DRM system in accordance with the present invention may be operated, one or more of the steps may take place in a different order, or approximately simultaneously.

[0040] In an embodiment where distribution point 128 is an application within a mail server, distribution point 128 may be operated to intercept incoming protected content to protect its access, and to make a request to license server 110 for a license for one or more end users 114 who are subscribers. Distribution point 128 may then pre-package the protected

content and provide the pre-packaged content to the mail server workflow so that the mail server can route the protected content to the end users.

[0041] In an embodiment where distribution point 128 is integrated with subscriber list manager 120, public keys associated with end users 114 and maintained as a list of end user's identities are typically, but not necessarily, uploaded from client 106 during the activation process with activation server 102. In addition, in an enterprise, subscription list manager 120 may be integrated with a directory services system or similar system. The list of end users may also include a list of content that each of the end users subscribe to, in addition to the identity information and public keys.

[0042] Moreover, access to protected content may be through a pull model where end users pro-actively seek and use protected content such as by downloading protected content from a web site. Alternatively, access to protected content may be through a push model where end users receive protected content through e-mail, e-mail attachment, or by other mechanism.

[0043] A significant advantage of DRM system 100 is that it allows automation of the end user's access to a collection of protected content when the end user becomes a member of a designated subscription group for a particular subscription. Various end users can subscribe and unsubscribe and the subscription list may be managed by the end users themselves, or managed by another person or automated management system. Automation of the end user's access also allows the process for obtaining of a license for accessing particular protected content to be made transparent to the end user. For example, in the pull model, an end user may make downloads or otherwise access plurality of protected content without additional transaction steps to obtain required software or licenses for each of the protected content accessed after the initial activation. In the push model, the end user receives the protected content through e-mail, e-mail attachment, or by another

mechanism which can be opened without any additional transaction steps after the initial activation.

[0044] It should be noted that actual delivery of the license and/or the protected content may be performed in various ways, for instance, by specialized systems such as delivery engines. Delivery engines are specialized and highly efficient entities that deliver content to a large population. For example, delivery engines may be used by a brokerage firm to deliver stock transaction confirmations by outsourcing this task to a company that specializes in low cost delivery of such documents.

[0045] Examples of specific types of subscriptions may be provided for use with the preferred embodiment are "subscribe-and-rent" subscriptions, and "subscribe-and-acquire" subscriptions. In subscribe-and-rent subscriptions, an end user is only allowed to access protected content while being an active subscriber, or based on some other condition, for example, a time period, a number of views, or until the next version of the content is made available. One example of a subscribe-and-rent subscription type is for online use of streaming media. Typically, protected content would be used on-line and once the subscription expires or a period of time lapses, the protected content, including previously accessible content, as well as unaccessed content is no longer made available to the end user. In this type of subscription usage rights, conditions, and state variables can be used to limit the manner of use in a known manner.

[0046] In subscribe-and-acquire subscriptions, end users actually acquire protected content. For instance, a certain amount or type of protected content could be acquired from a larger collection comprising a plurality of protected content. In addition, there could be preferential pricing, access, or terms can be given to a subscribing and user. In subscribe-and-acquire subscriptions, once the protected content is legitimately acquired, an end user would have the right to use it indefinitely and expiration of the subscription does not

generally terminate the right to use content previously acquired. Business documents such as stock transaction confirmations are a typical example of a protected document appropriate for subscribe-and-acquire subscription.

[0047] Of course, in other implementations, both subscription types can be combined. For example, a subscribing end user may be offered a package that includes on-line access to all protected content and a predetermined number of downloads. In a music application, a subscribing end user may have on-line access to the entire catalog of music titles, but only be allowed to download one hundred titles. Of course, other permutations and subscription models are possible in implementing a subscription based DRM system and method. For instance, in another example, a subscription based DRM system and method would allow rights to a specific number, for example one hundred, downloads to be deferred, accumulated, or transferred to another person, or even returned to the subscription provider. Also, for example, acquisition could be made to persist only for the duration of certain conditions and does not literally have to be for an indefinite period.

[0048] In addition, different subscription models may be apply to different parts of the protected content. For example, a periodical may be acquired on a subscribe-and-acquire basis, but images that are part of the periodical may be acquired on a subscribe-and-rent basis and thus might expire or require additional fees for example. The license associated with the particular protected content could define the different treatment between the periodical itself and the images thereof. Once downloaded, protected content may be accessed and used by the end user off-line in the manner determined by the license associated with the protected content. With a combination of on-line and off-line subscription, many models can be constructed using the subscription based DRM system and method of the present invention.

[0049] As an example, a subscription based DRM system may be used in a storefront application. A storefront may be any on-line e-commerce site that

offers protected content for sale. In this regard, distribution point 128 shown in DRM system 100 of Fig. 2 may be such a storefront. End user 114 activates client 106 and obtains public and private keys. The end user then joins a subscription list by responding to a subscription offer in the storefront and makes payment, or satisfies other conditions. Subscription list manager 120 pulls each public key and associates the public key with end user's identity. End user then attempts to download protected content such as a document that is part of a subscription collection. The storefront validates the end user's membership to the subscription through subscription list manager 120, retrieves end user's public key from subscription list manager 120, and makes a request to license server 110 for the licenses associated to the requested protected content. License server 110, after verifying authenticity of the request, issues licenses 116 to the storefront. The storefront then pre-packages the license with protected content 108 and makes it available for download by end user 114 as discussed previously. End user 114 can then download protected content 108 and transparently use protected content 108 in the manner dictated by issued license.

[0050] In another example, a subscription based DRM system and method of the present invention may be used in a delivery engine application that provides secure delivery of protected content such as documents. For instance, end users 114 may sign up as a subscriber to content 108 provided by Company A that owns or controls content 108, and activates a client via activation server 102 to obtain keys. Company A works with Company B that offers a secure digital delivery service to outsource the document delivery portion of its subscription service offering. The outsourced document delivery may be for delivery of financial statements or other type of documentation requiring protection and restricted use. Such outsourcing may be beneficial to Company A because Company B may be more efficient and cost effective in this particular function of document delivery. Company B thus serves as a "delivery engine" controls subscription list manager 102 to manage the list of

end users 114 that receive documents, i.e. a subscription list which associates subscribing customers of Company A with their public key obtained during the activation stage. Of course, there could be more than one subscription list, for example a list of preferred customers, a list of specific types of customers, and the like.

[0051] When Company A has a document to deliver to its subscribers, it prepares the document and provides it to Company B for delivery. Company A then instructs Company B to deliver the document to users in one or more subscription list(s), for example, to most preferred customers. Company B sends a request to license server 110 to issue licenses 116 for each customer, i.e. user 114 in the list of most preferred customers, each customer being associated with a particular public key. Once requested licenses 116 are issued by license server 110, Company B receives licenses 116, pre-packages the documents with the licenses 116', and delivers them to the subscribing customers in the most preferred customer list. Because the documents are pre-packaged 116' with the required license, the subscribing customers need not conduct an additional transaction to use the protected content in accordance with the license 116. Thus, each end user that receives the pre-packaged license can receive and access the protected document transparently without further activations.

[0052] Another example of the subscription based DRM system and method is in an enterprise application. Distribution point 128 in such an application may be a computer application that is integrated with a mail server, or other application of the enterprise. Additionally, the enterprise application may maintain the subscription list in any appropriate manner as previously described. In this enterprise application example, end users 118 such as Person A, Person B, and Person C, are activated through activation server 122. When Person A sends a protected document to Person B and Person C, distribution point 128 intercepts the document and makes a request

to license server 110 for a license 116 on behalf of Person B and Person C. Distribution point 128 then retrieves public keys for Person B and Person C and uploads the public keys to license server 110 which issues licenses 116 granting Person B and Person C rights to the protected document sent by Person A.

[0053] Once licenses 116 are received from license server 110, distribution point 128 pre-packages the protected document with the issued license 1161 and inserts it to the normal mail server workflow so that the mail server routes the protected document to Person C and Person B. Both Person B and Person C can then access and use the received document transparently when they check their respective e-mails in accordance with the issued license.

[0054] Another example of subscription based DRM system and method is a digital music store application. In such an application, a music company, for instance, an online music store, may offer a subscription to customers as users 114 where for a predetermined fee, users 114 are allowed access to unlimited (or limited) on-line streaming use of the music store's music catalog titles, and download a predetermined number of music titles.

[0055] When a subscribing user 114 seeks to access the music store's music catalog, DRM system authenticates the subscribing user 114 with activation server 102 and ensures that the user is identified in a subscription list of subscription list manager 120 before allowing access to the music catalog and the titles therein. As the user downloads various music titles as content 108, from the music store, license server 110 can keep track of the number of titles user 114 has downloaded so that if the maximum number of downloads has not been exceeded, the music store sends a request to the license server to generate licenses 116 for the selected titles. Once license server 110 issues the required licenses, the online music store pre-packages the protected title with the appropriate license 116 using a document

packaging application. The user can then transparently download the selected titles from the music store.

[0056] Further, the subscription based license of the preferred embodiment permits activation prior to the existence of the content. For example, a user can subscribe to receive a live streaming event prior to the event.

[0057] It should again be understood that whereas the terms "server" and "client" are used to describe the devices for implementing the present invention in the illustrated embodiments above, these terms should be broadly understood to mean any appropriate device or devices for executing the described function.

[0058] Communication between the various devices can be accomplished through any channel, such as a local area network (LAN), the Internet, serial communications ports, and the like. The communications channels can use wireless technology, such as radio frequency or infra-red technology. The various elements of the preferred embodiment such as the various servers and databases connected thereto are segregated by function for the purpose of clarity. However, the various elements can be combined into one device or segregated in a different manner. For example, software package, and public and private key pair can be a single executable file and data files, or plural files or modules stored on the same device or on different devices. The software package can be any exchange of information that permits license activation and need not include a rendering application, a public key can be any type of identification tag or code. Further, the function of the various devices can be combined. For example, a single device can accomplish the function of license server 110 activation server 102, subscription list manager 120, and client 106. Also, the functions can be combined or segregated into any number and configuration of devices. The various components and modules have separate utility and may exist alone or in combination.

[0059] Any protocols, data types, or data structures can be used in accordance with the invention. Moreover, any appropriate means of expressing usage rights and conditions may be used in implementing the present invention. For instance, as previously noted, a rights language, e.g. a grammar such as XrML™ can be used.

[0060] While various embodiments in accordance with the present invention have been shown and described, it is understood that the invention is not limited thereto. The present invention may be changed, modified and further applied by those skilled in the art. Therefore, this invention is not limited to the detail shown and described previously, but also includes all such changes and modifications as are encompassed by the appended claims and legal equivalents.

What is claimed:

1. A rights management system for managing use of items having usage rights associated therewith, said system comprising:

an activation device adapted to issue a software package that enforces usage rights to control use of said items, said software package including an identification mechanism associated with a user;

a user device adapted to receive said software package, receive a license having usage rights specifying a manner of use and being associated with at least one item, and allow said user to access said at least one item in accordance with said license;

a subscription managing device including a subscription list having said identification mechanism associated with subscribed users;

means for receiving a license request for a requested item on behalf of at least one user; and

a license device adapted to issue said license associated with said at least one item, said license device communicating with said subscription managing device and verifying that said identification mechanism for said at least one user is in said subscription list prior to issuing said license.

2. The rights management system of claim 1, wherein said at least one user is a plurality of users, each of said users having a public key as said identification mechanism.

3. The rights management system of claim 2, wherein said subscription managing device maintains a list of the identity of subscribed users via said public key associated with each of said users.

4. The rights management system of claim 3, wherein said at least one items is a plurality of items of protected content.

5. The rights management system of claim 4, wherein said plurality of items of protected content comprise at least one of a text file, an audio file, a video file, and digital multimedia files.

6. The rights management system of claim 1, wherein said at least one item is a plurality of items of protected content.

7. The rights management system of claim 4, further including a distribution point adapted to pre-package said license from said license device with said at least one item for each user in said subscription list.

8. The rights management system of claim 7, wherein said distribution point is further adapted to count the number of items accessed by said at least one user.

9. The rights management system of claim 8, wherein said subscription managing device is further adapted to remove said at least one

user from said subscription list when a predetermined number of items is accessed by said at least one user.

10. The rights management system of claim 8, wherein said distribution point is an on-line storefront application.

11. The rights management system of claim 1, wherein said subscription managing device also includes a mail server directory.

12. A method for managing use of items having usage rights associated therewith, said method comprising the steps of:

providing a software package to at least one user, said software package enforcing usage rights to control use of said items and having an identification mechanism associated with said at least one user;

storing said identification mechanism associated with said at least one user in a subscription list corresponding to said at least one item;

receiving a request from said at least one user to access said at least one item;

verifying that said at least one user requesting access to said at least one item is listed in said subscription list; and

issuing a license that grants usage rights to said at least one user to use said at least one item if said user is in said subscription list.

13. The method of claim 12, wherein said at least one item is a plurality of items of protected content adapted to be accessed by said at least one user.

14. The method of claim 13, wherein said at least one user is plural users and further comprising the step of issuing a plurality of licenses granting usage rights to each of said plural users to use said plurality of item of protected content.

15. The method of claim 14, further comprising the step of verifying that each of said plural uses are listed in said subscription list prior to issuing each license that grants usage right to use each of said plurality of protected content.

16. The method of claim 13, further comprising the step of counting the number of items of protected content used by each of said plural users.

17. The method of claim 16, further comprising the step of removing said identification mechanism associated with a user when a predetermined number of items of protected content is used by that user.

18. The method of claim 12, wherein said identification mechanism is a public key.

19. The method of claim 18, further comprising the step of verifying that a public key of a user requesting access to a particular item of protected content is listed in said subscription list prior to issuing a license that grants usage rights to that user to use said particular item of protected content.

20. The method of claim 11, further comprising the step of pre-packaging said issued license together with said at least one item for each user in the subscription list.

21. A method of subscribing a user for access to protected item, said method comprising:

issuing a private key and a public key to users;

adding the public key of the users to a subscription list corresponding to items of protected content; and

packaging a license to one of the items of protected content upon receipt of a request for said one of the items for protected content and verification that the public key of a user making the request is a public key that is in the subscription list.

Fig. 1

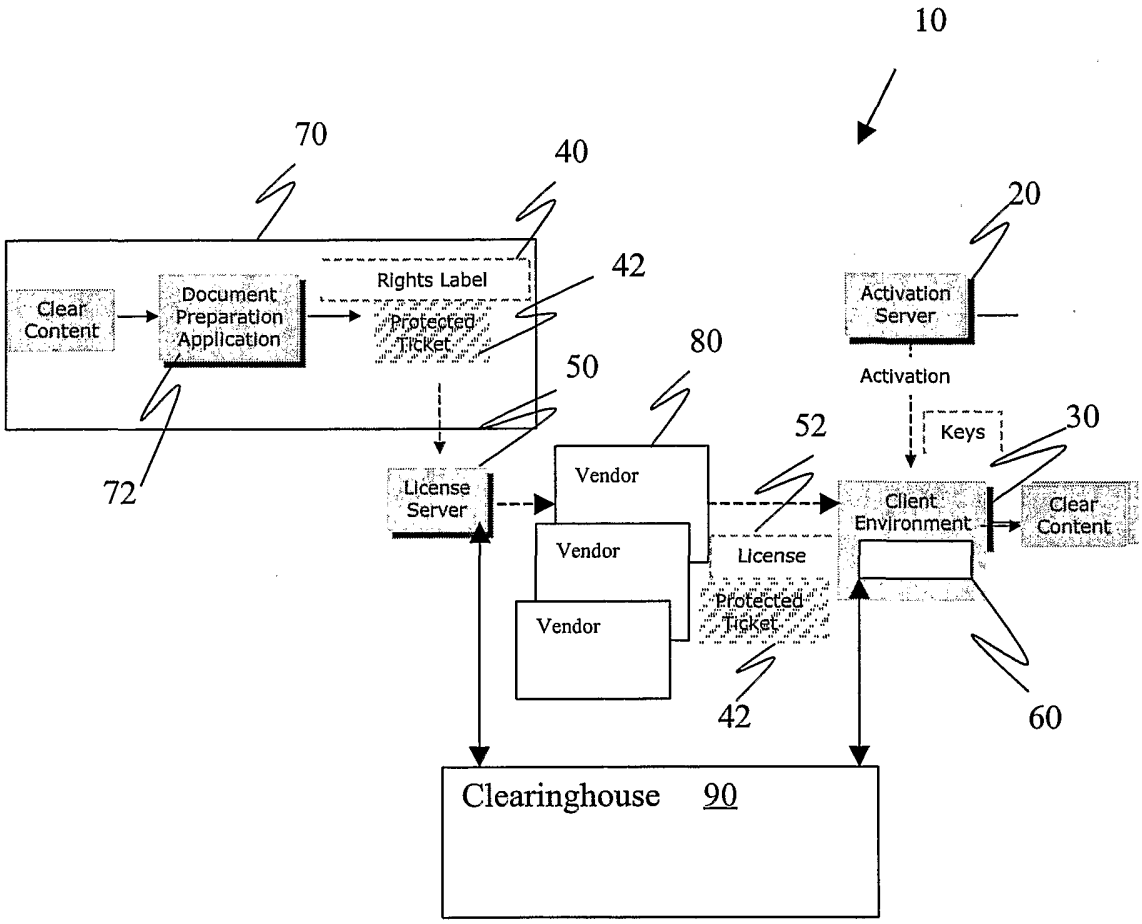

10
70
40
20
42
Clear Content
Document Preparation Application
Rights Label
Protected Ticket
Activation Server
Activation
80
50
52
Keys
30
72
License Server
Vendor
Vendor
Vendor
License
Protected Ticket
Client Environment
Clear Content
42
60
Clearinghouse 90

Fig. 2

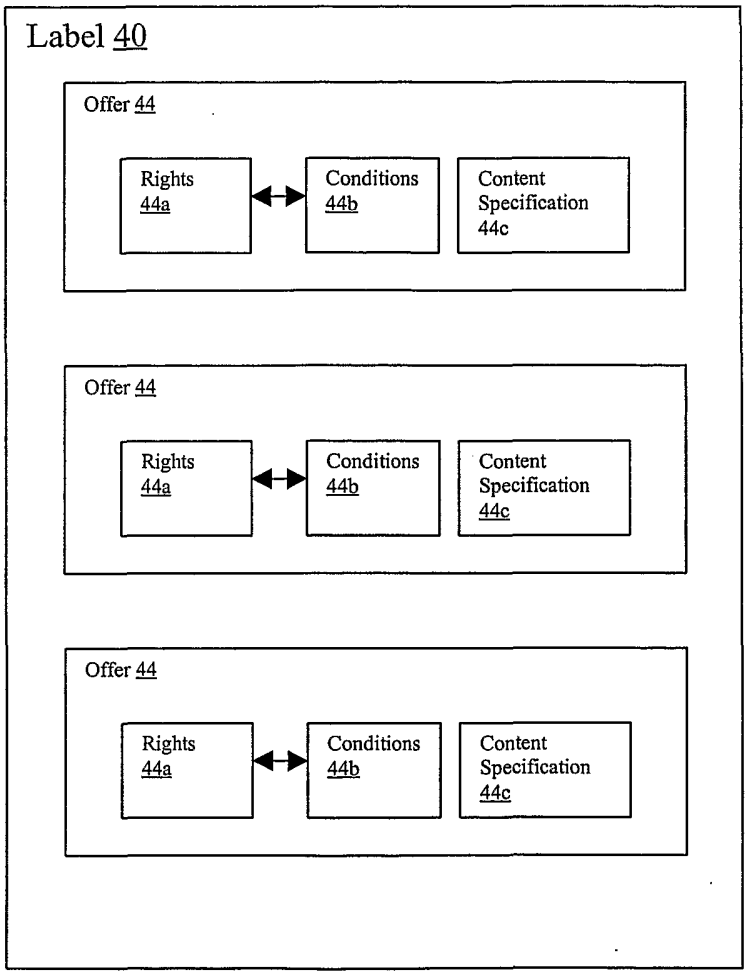

Label 40
Offer 44
Rights 44a
Conditions 44b
Content Specification 44c
Offer 44
Rights 44a
Conditions 44b
Content Specification 44c
Offer 44
Rights 44a
Conditions 44b
Content Specification 44c

Fig. 3

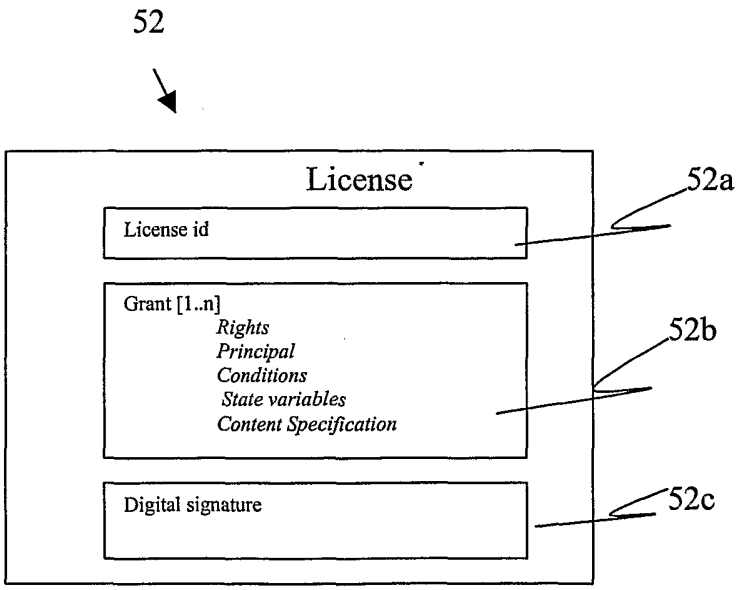

52
License
License id
Grant [1..n]
Rights
Principal
Conditions
State variables
Content Specification
Digital signature
52a
52b
52c

Fig. 4

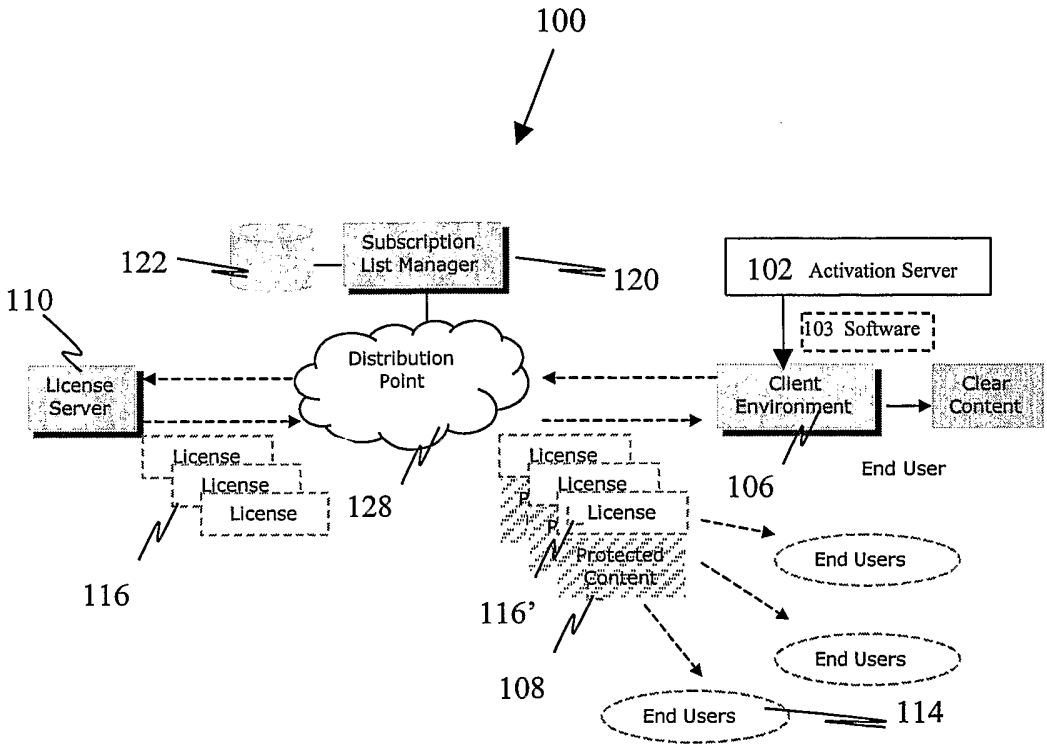
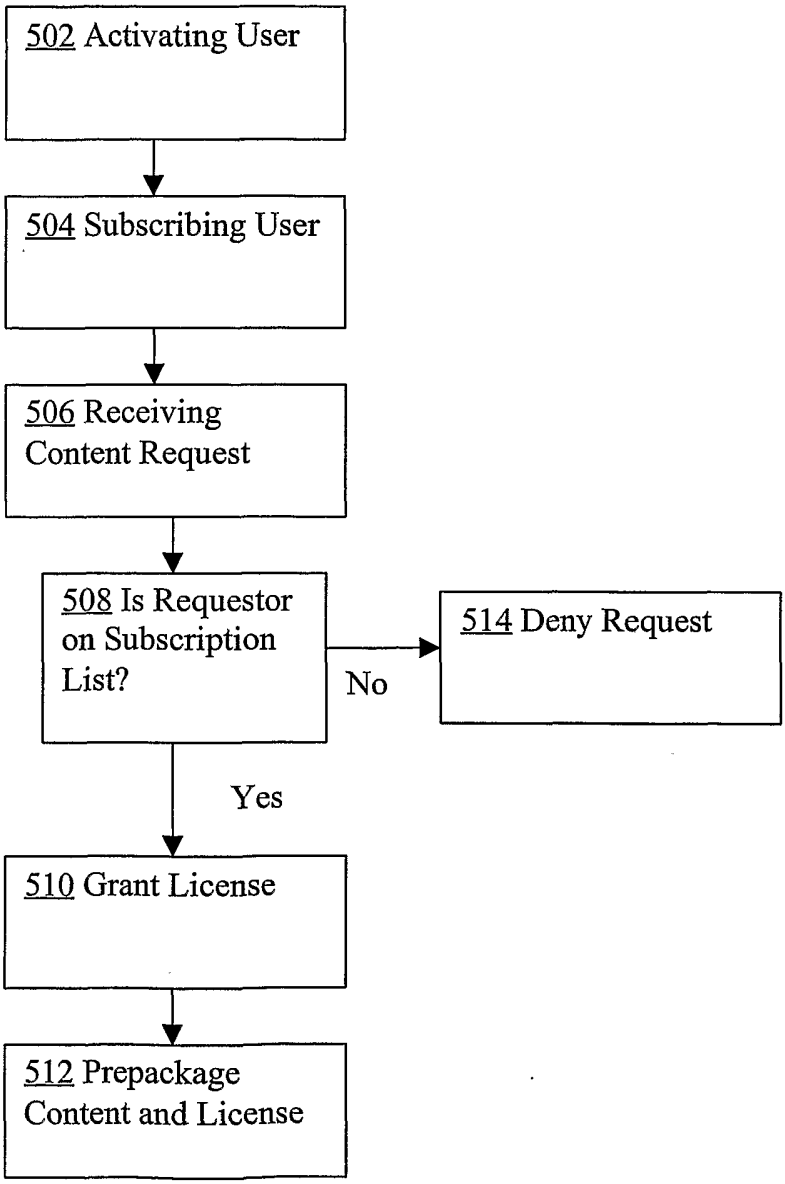

100
122
Subscription List Manager
120
102 Activation Server
103 Software
110
License Server
Distribution Point
Client Environment
Clear Content
End User
106
License
License
License
128
116
License
License
License
Protected Content
116'
108
End Users
End Users
End Users
114

Fig. 5


502 Activating User
504 Subscribing User
506 Receiving Content Request
508 Is Requestor on Subscription List?
No
514 Deny Request
Yes
510 Grant License
512 Prepackage Content and License

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US02/17851

A. CLASSIFICATION OF SUBJECT MATTER

IPC(7) : G06F 17/00
US CL : 235/375

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
U.S. : 235/375, 382; 705/17, 18, 59

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
NONE

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
NONE

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 6,189,146 B1 (MISRA et al) 13 February 2001 (13.02.2001), column 2, lines 12-61; column 3 line 59 - column 4, line 67; column 6, line 21 - column 7 line 25; column 11, line 46 - column 12, line 15.	1-10, 12-21
Y	US 6,169,976 B1 (COLOSSO) 02 January 2001 (02.01.2001), column 4, line 52 - column 5, line 40; column 8 line 18 - column 10, line 40; column 12, lines 19-37; column 14, line 15 - column 16, line 56.	1, 11
Y	US 5,745,879 (WYMAN) 28 April 1998 (28.04.1998) column 8, lines 22-44; column 9, lines 22-44.	1, 11
A	US 6,216,112 B1 (FULLER et al) 10 April 2001 (10.04.2001), column 2, line 50 - column 3, line 45.	1-21
A	US 6,219,652 B1 (CARTER et al) 17 April 2001 (17.04.2001), column 4, line 39 - column 7, line 10.	1-21

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
22 July 2002 (22.07.2002)	03 OCT 2002
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703) 305-3230	Authorized officer Lisa M Caputo Telephone No. (703) 305-3503

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