US 20140380436A1

(19) United States

(12) Patent Application Publication

(10) Pub. No.: US 2014/0380436 A1

(43) Pub. Date: Dec. 25, 2014

Padhye et al.

(54) **DIGITAL RIGHTS MANAGEMENT OF CONTENT WHEN CONTENT IS A FUTURE LIVE EVENT**

(71) Applicant: **CONTENTGUARD HOLDINGS, INC.**, Plano, TX (US)

(72) Inventors: **Tushar N. Padhye**, Hosur (IN); **M.S. Roopa**, Banagalore (IN); **C.V. Joshi**, Bangalore (IN); **Basavaraj B.H.**, Bangalore (IN); **Arun Ray**, Bangalore (IN); **Deepanjan Kanungo**, Bangalore (IN); **Aram Nahidipour**, Laguna Niguel, CA (US); **Xin Wang**, Torrance, CA (US); **Thanh Ta**, Huntington Beach, CA (US); **Michael Raley**, Downey, CA (US); **Guillermo Lao**, Torrance, CA (US); **Eddie Chen**, Rancho Palos Verdes, CA (US); **Bijan Tadayon**, Germantown, MD (US); **Anant Kansal**, Bangalore (IN)

(21) Appl. No.: **14/481,453**

(22) Filed: **Sep. 9, 2014**

Related U.S. Application Data

(63) Continuation of application No. 13/329,640, filed on Dec. 19, 2011, now Pat. No. 8,862,517, which is a continuation of application No. 10/162,699, filed on Jun. 6, 2002, now Pat. No. 8,099,364, which is a continuation-in-part of application No. 09/867,747, filed on May 31, 2001, now Pat. No. 6,876,984.

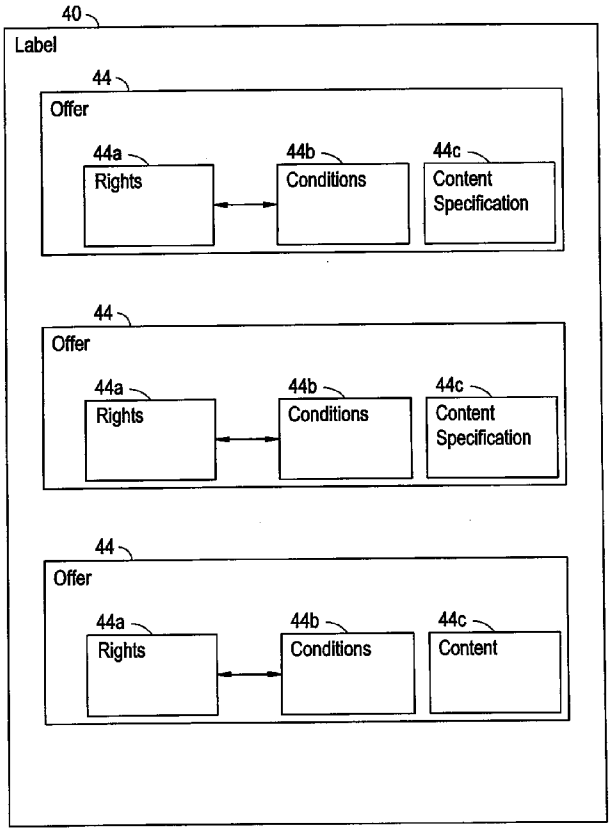
Publication Classification

(51) **Int. Cl.**
H04L 29/06 (2006.01)

(52) **U.S. Cl.**
CPC ***H04L 63/10*** (2013.01); ***H04L 65/60*** (2013.01)
USPC **726/4**

(57) **ABSTRACT**

A method and system for managing use of items having usage rights associated therewith including a point of capture system adapted to generate content of a future event when the event occurs, a content distributor adapted to generate a rights label having usage rights associated with content of the future event before the content is created, the rights label having a distribution key for encrypting the content as the content is generated, the distribution key being encrypted with a public key. The system also includes a license server adapted to generate a license associate with the content from the rights label before the content is generated, the license including the distribution key encrypted with the public key, and a content distributor adapted to distribute the license before the content is generated.



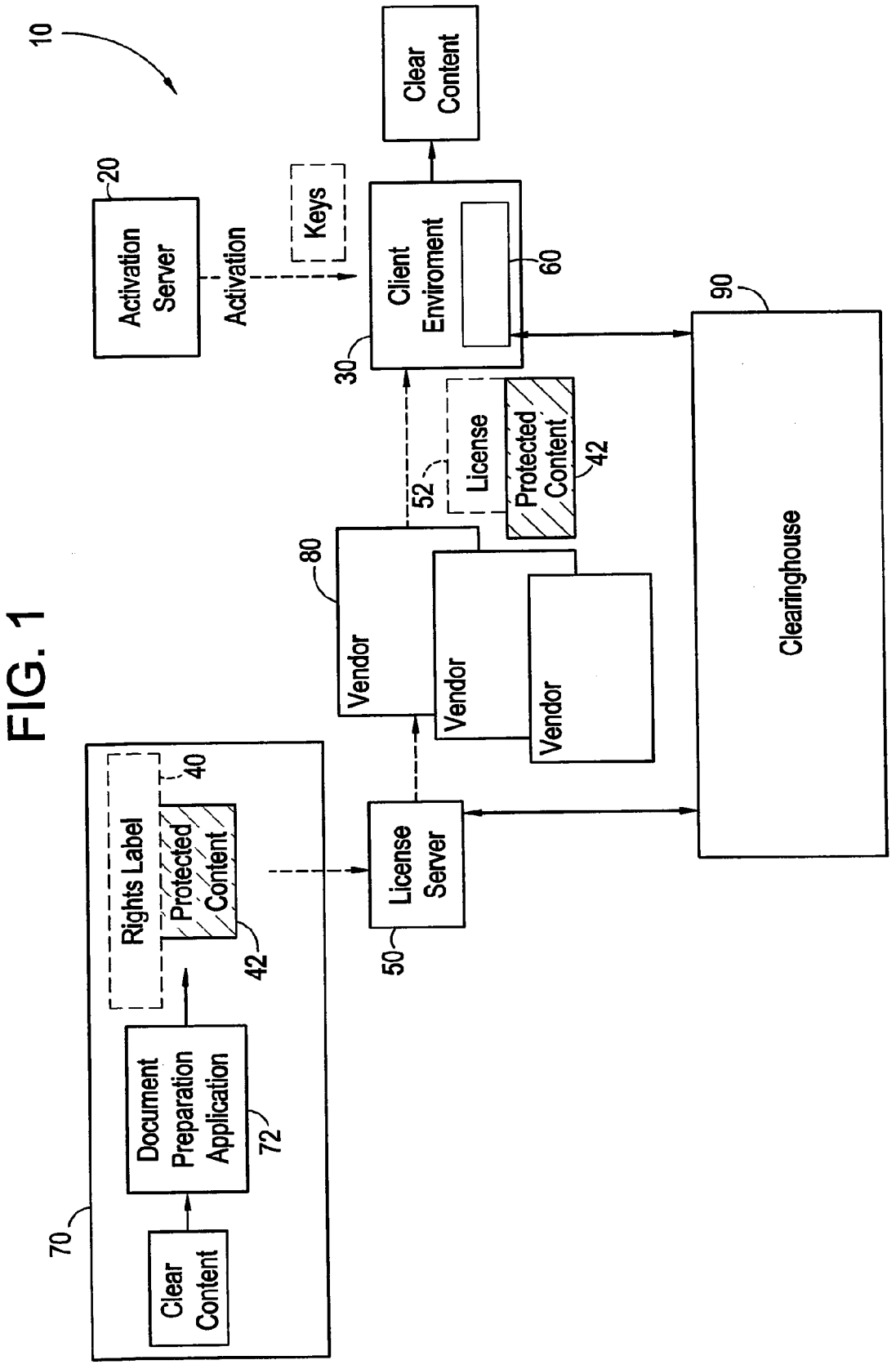

10
Clear Content
20
Activation Server
Activation
Keys
Client Enviroment
60
30
90
License
Protected Content
42
52
80
Vendor
Vendor
Vendor
Clearinghouse
Rights Label
40
Protected Content
42
License Server
50
Document Preparation Application
72
Clear Content
70

FIG. 1

FIG. 2

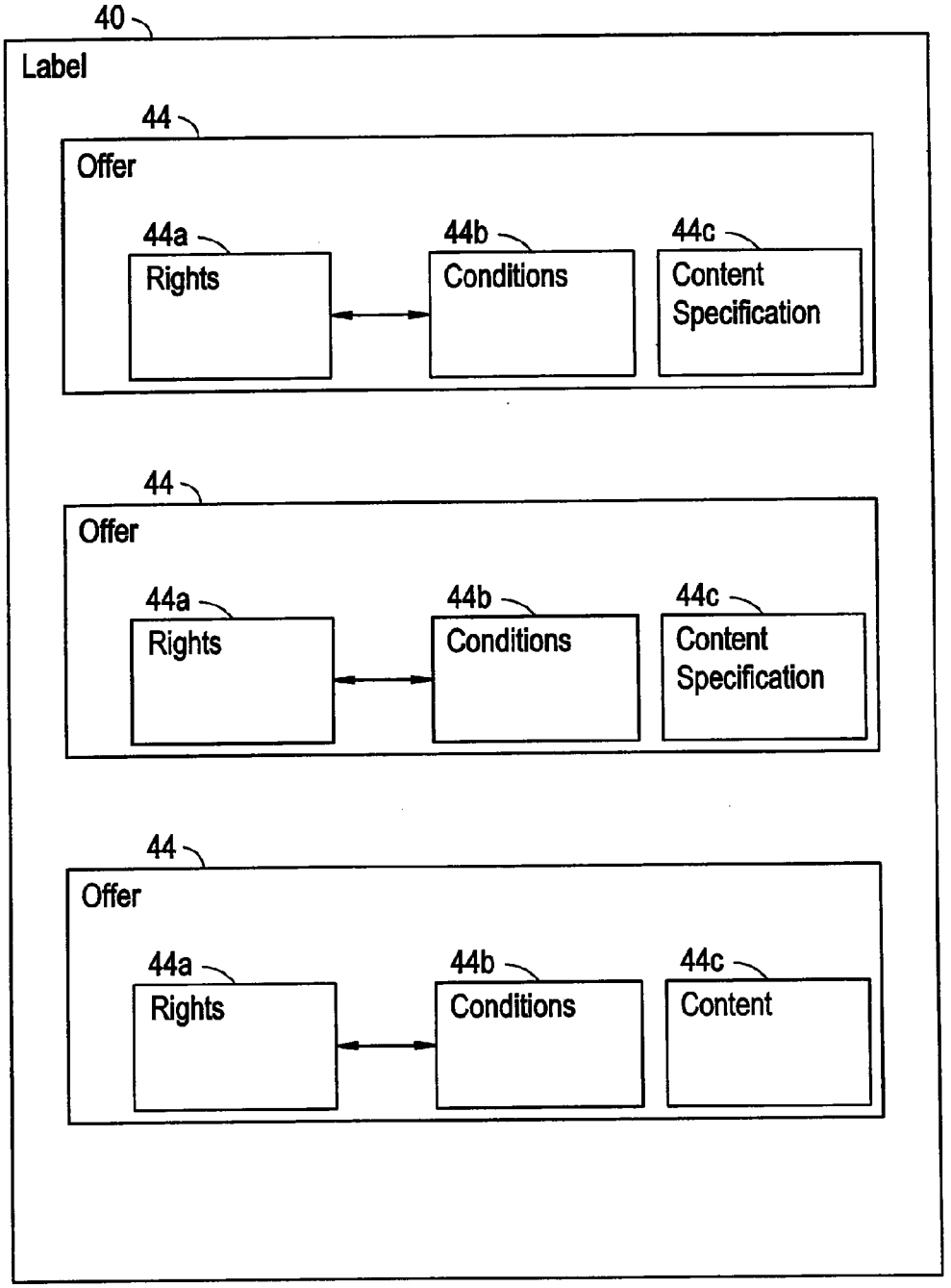

40
Label
44
Offer
44a
Rights
44b
Conditions
44c
Content Specification
44
Offer
44a
Rights
44b
Conditions
44c
Content Specification
44
Offer
44a
Rights
44b
Conditions
44c
Content

FIG. 3

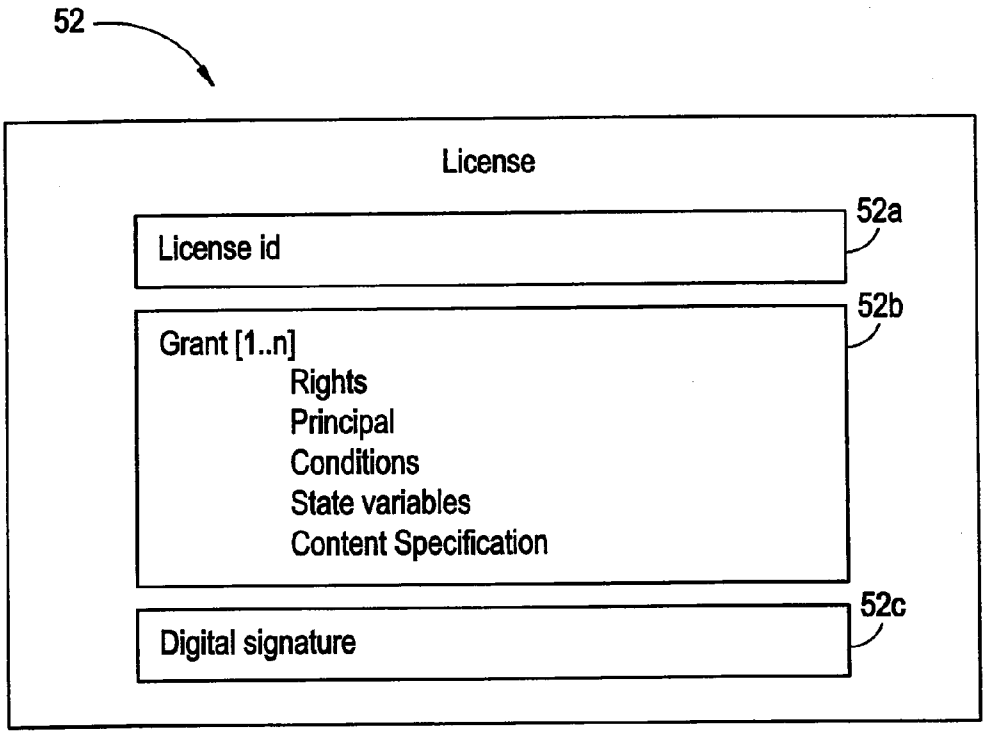

52
License
License id
52a
Grant [1..n]
Rights
Principal
Conditions
State variables
Content Specification
52b
Digital signature
52c

FIG. 4

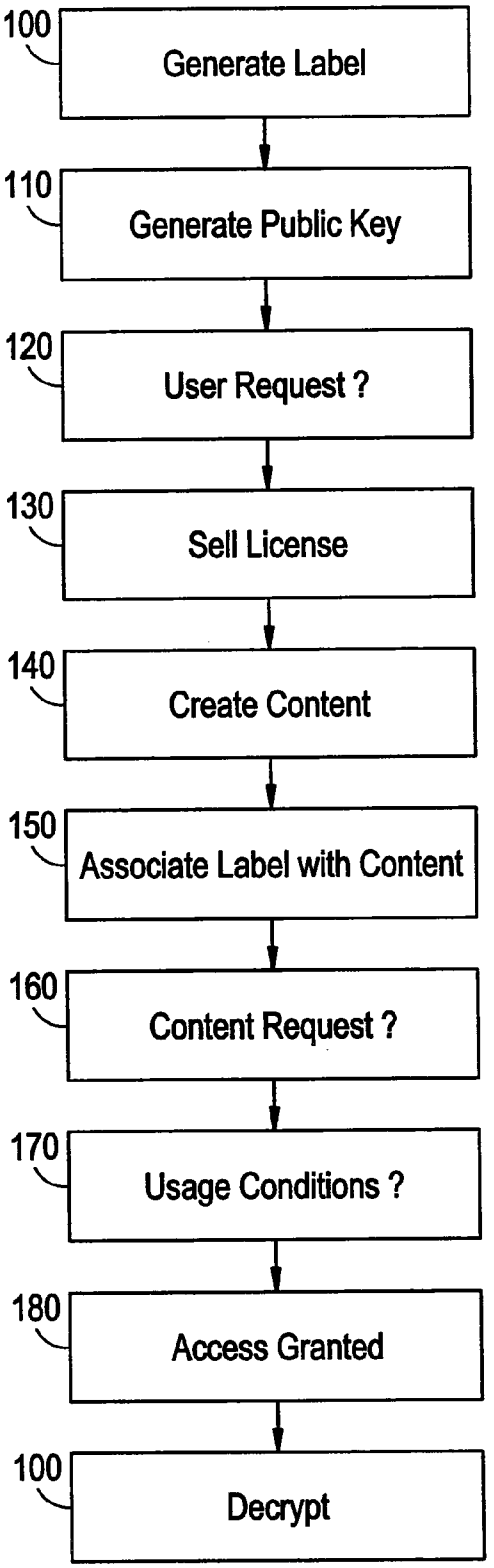

100
Generate Label
110
Generate Public Key
120
User Request ?
130
Sell License
140
Create Content
150
Associate Label with Content
160
Content Request ?
170
Usage Conditions ?
180
Access Granted
100
Decrypt

FIG. 5

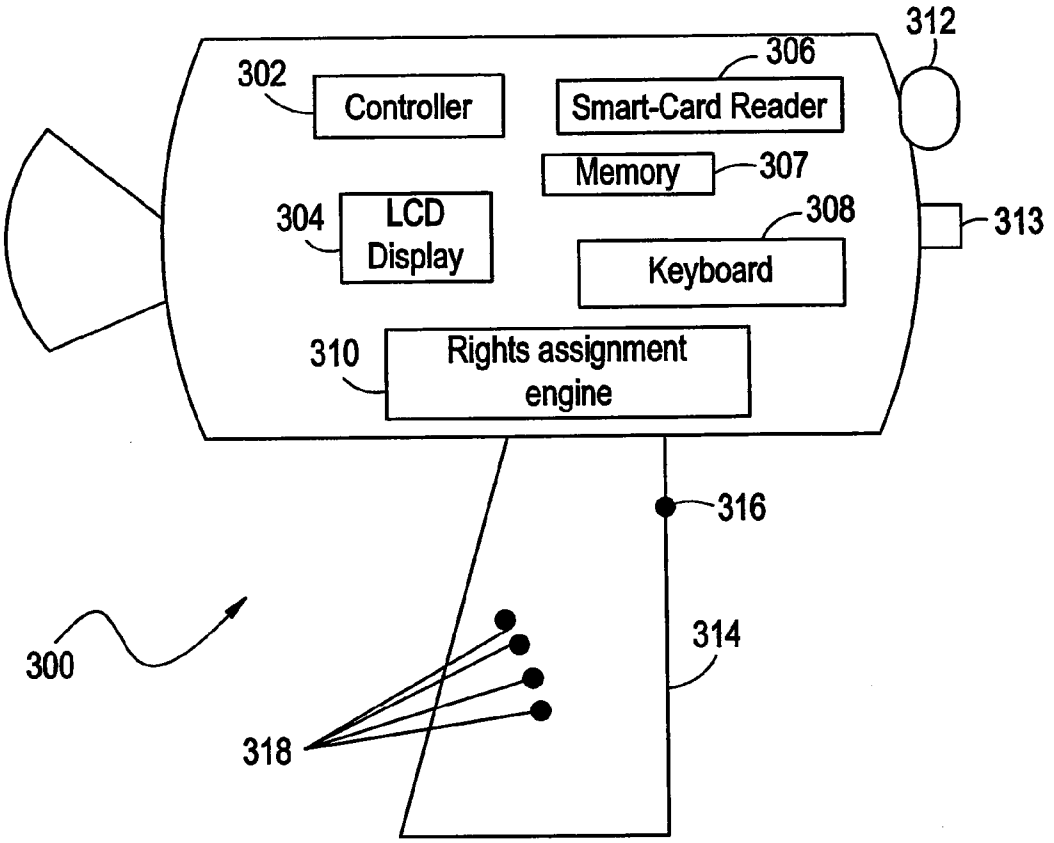

312
306
302
Controller
Smart-Card Reader
Memory
307
304
LCD Display
308
313
Keyboard
310
Rights assignment engine
316
314
300
318

FIG. 6

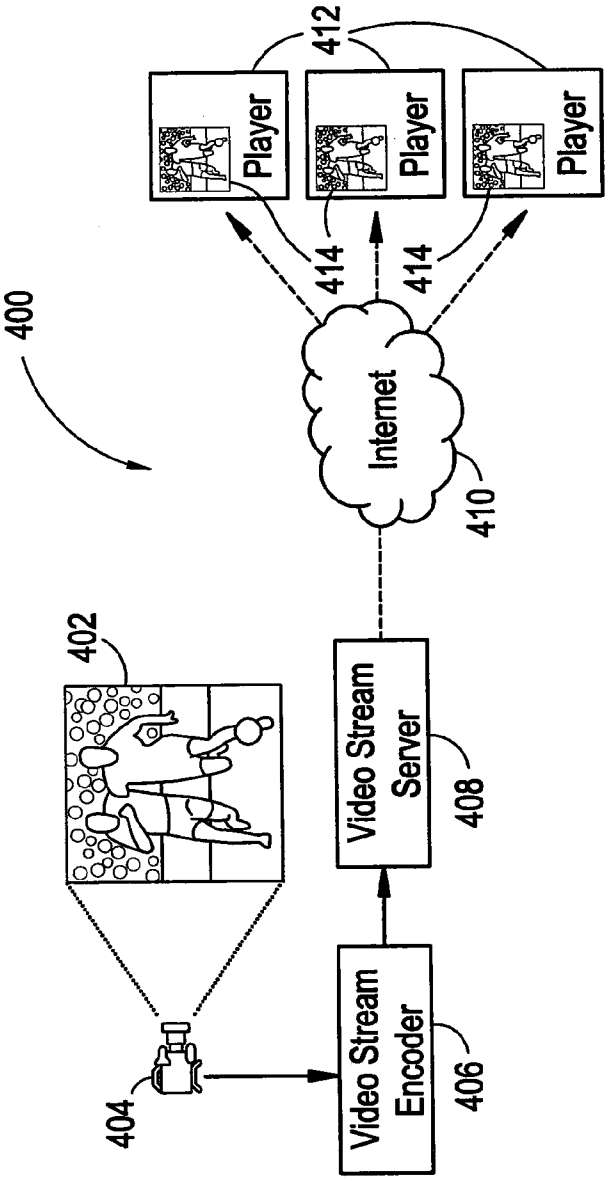

400
412
Player
Player
Player
414
414
Internet
410
402
Video Stream Server
408
Video Stream Encoder
406
404

FIG. 7

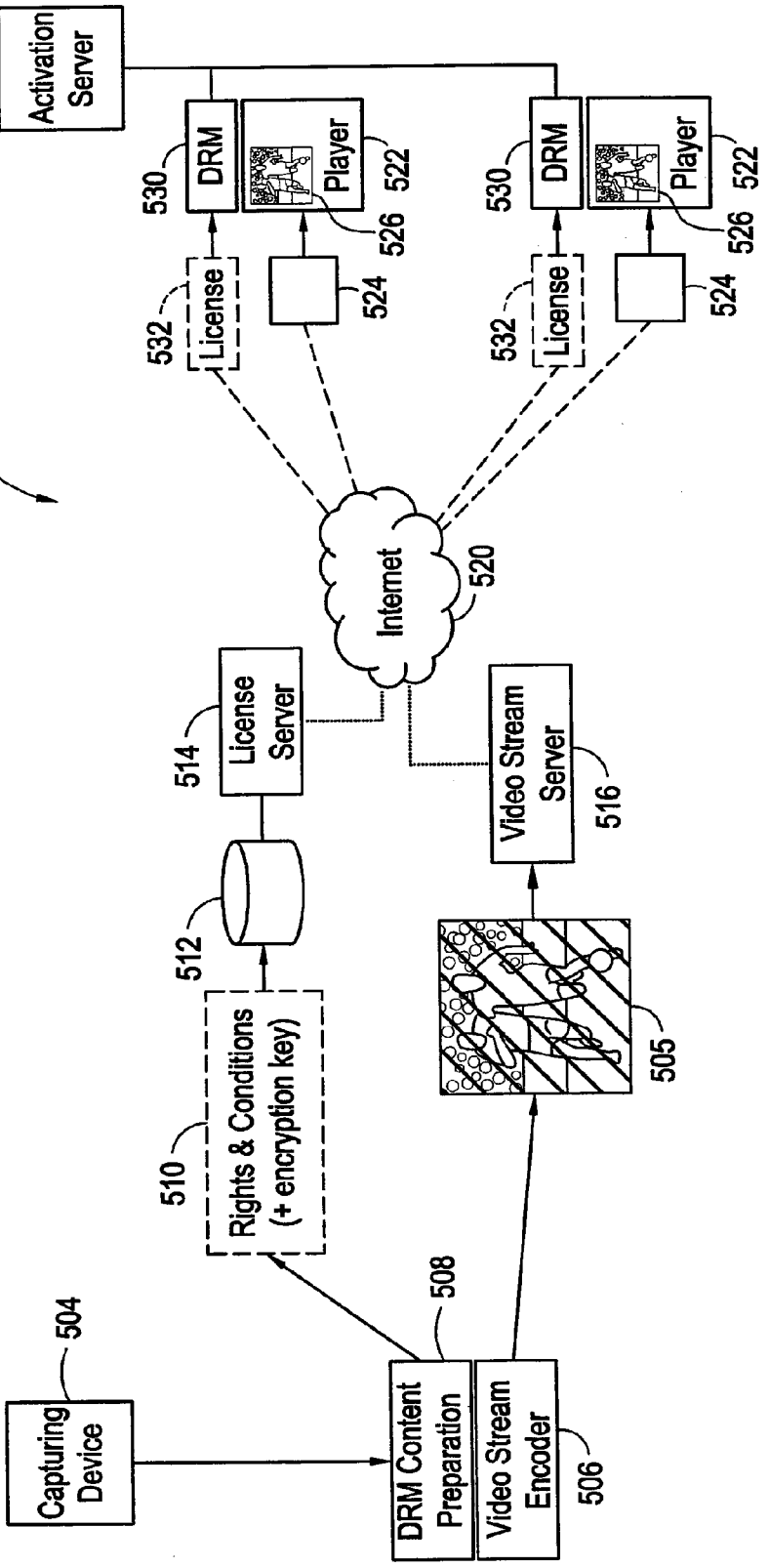

500
Activation Server
533
DRM
530
Player
522
526
License
532
524
Internet
520
License Server
514
Video Stream Server
516
512
Rights & Conditions (+ encryption key)
510
505
Capturing Device
504
DRM Content Preparation
Video Stream Encoder
508
506

FIG. 8

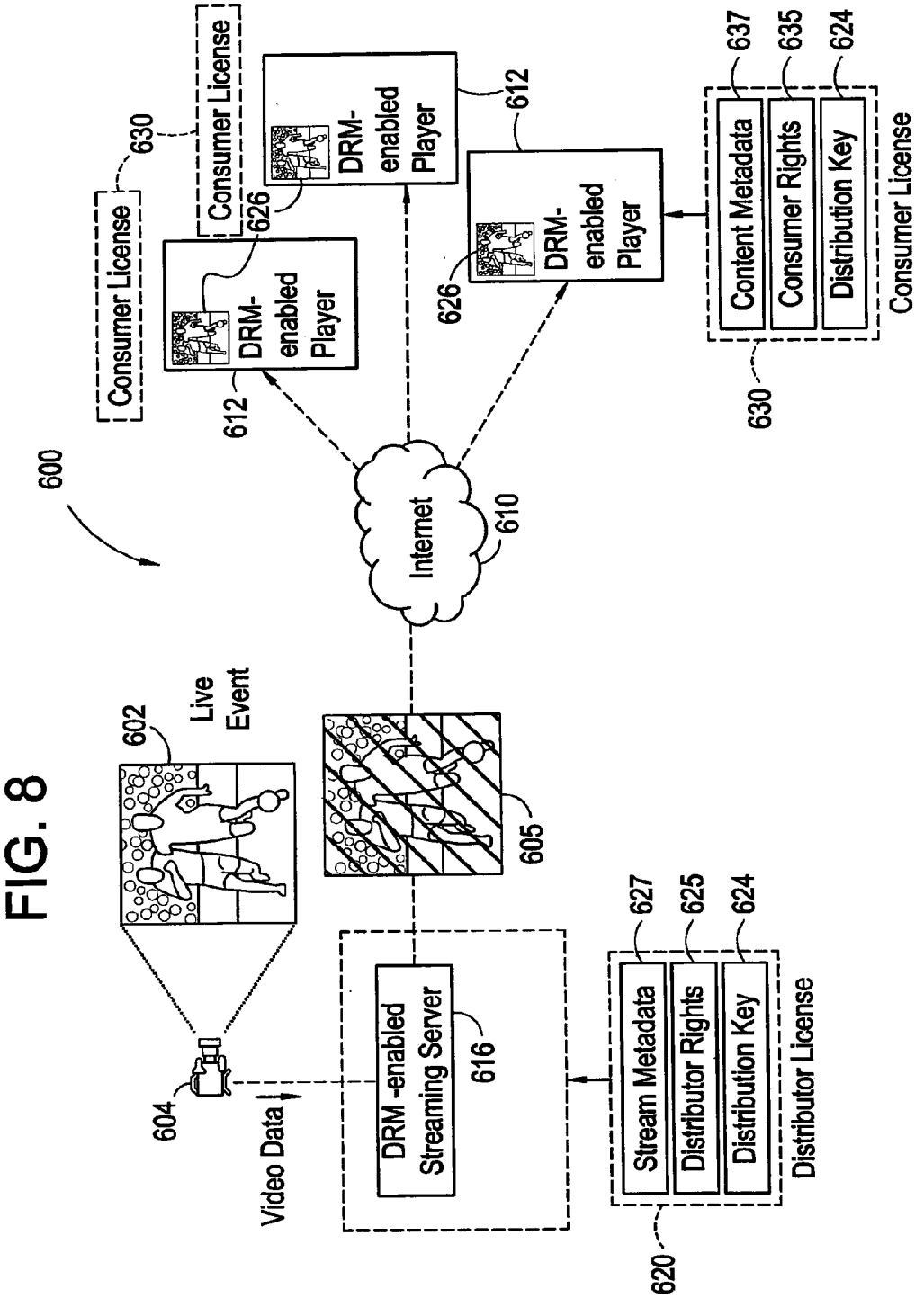

600
Live Event
602
604
Video Data
DRM -enabled Streaming Server
616
605
Internet
610
DRM-enabled Player
612
626
Consumer License
630
Content Metadata
Consumer Rights
Distribution Key
637
635
624
Consumer License
Stream Metadata
Distributor Rights
Distribution Key
627
625
624
Distributor License
620

FIG. 9

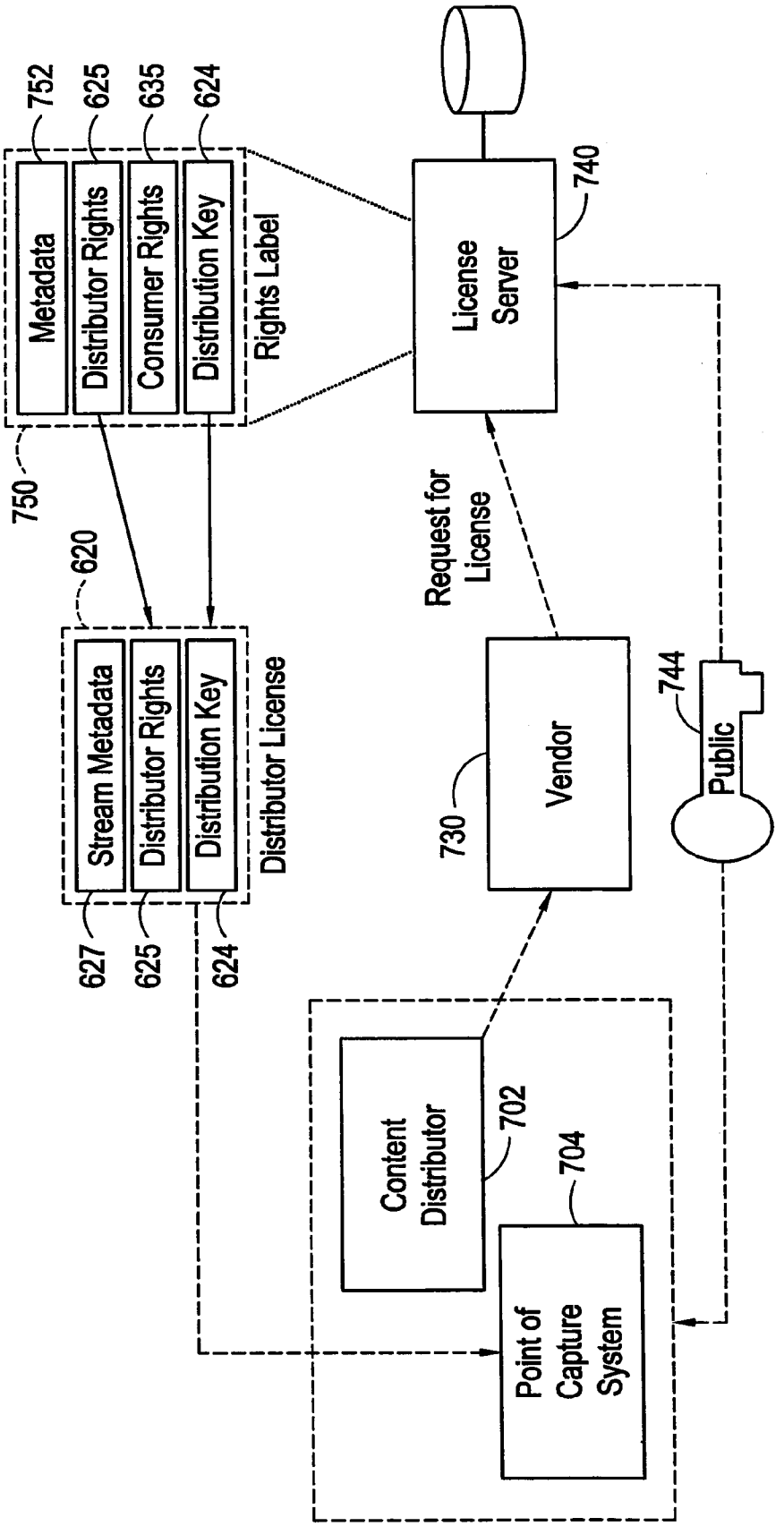

752
625
635
624
Metadata
Distributor Rights
Consumer Rights
Distribution Key
Rights Label
750
620
Stream Metadata
Distributor Rights
Distribution Key
Distributor License
627
625
624
License Server
740
Request for License
Vendor
730
744
Public
Content Distributor
702
704
Point of Capture System

FIG. 10

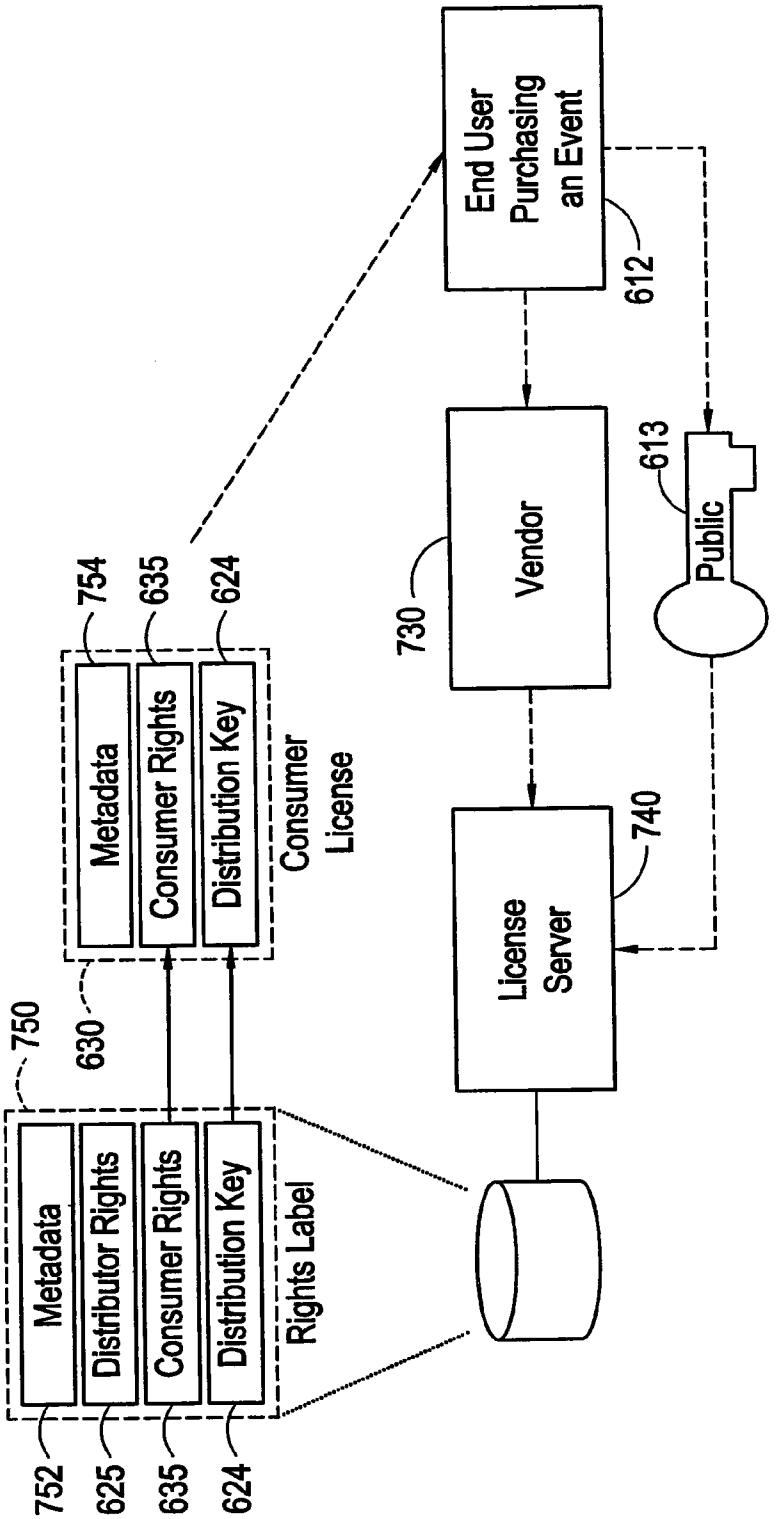
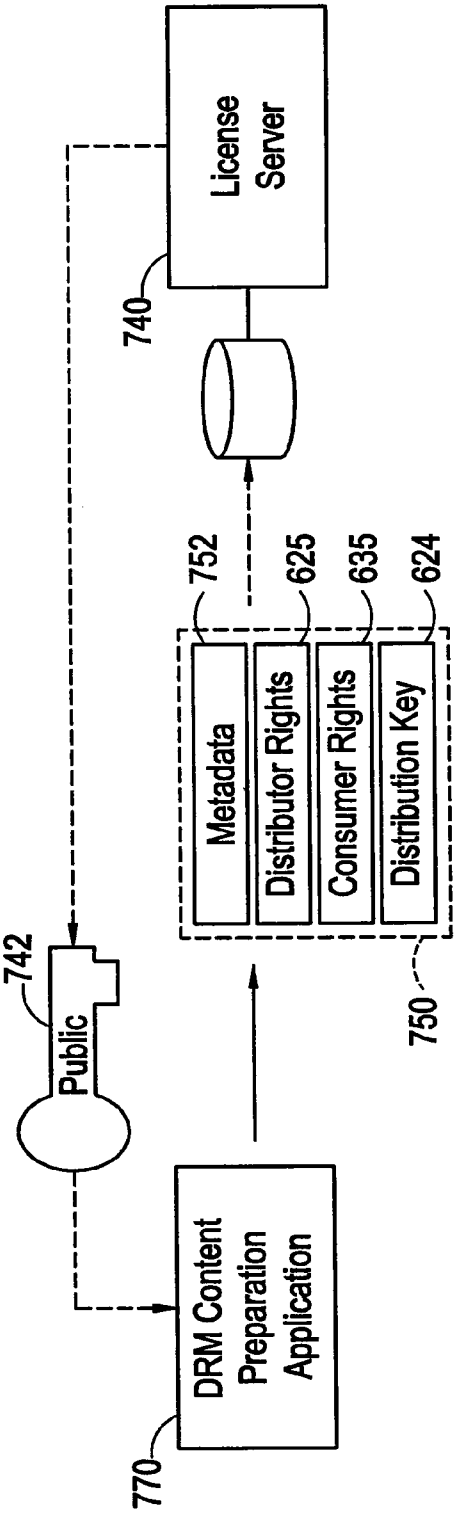

End User Purchasing an Event
612
Vendor
730
Public
613
License Server
740
Metadata
Consumer Rights
Distribution Key
Consumer License
754
635
624
630
750
Metadata
Distributor Rights
Consumer Rights
Distribution Key
Rights Label
752
625
635
624

FIG. 11


License Server
740
752
625
635
624
Metadata
Distributor Rights
Consumer Rights
Distribution Key
750
742
Public
DRM Content Preparation Application
770

DIGITAL RIGHTS MANAGEMENT OF CONTENT WHEN CONTENT IS A FUTURE LIVE EVENT

RELATED APPLICATION DATA

[0001] This application is a Continuation of U.S. patent application Ser. No. 13/329,640, filed Dec. 19, 2011, now allowed, which is a Continuation of U.S. patent application Ser. No. 10/162,699, filed Jun. 6, 2002, now U.S. Pat. No. 8,099,364, which is a Continuation-In-Part of U.S. patent application Ser. No. 09/867,747, filed May 31, 2001, now U.S. Pat. No. 6,876,984, and also claims benefit from U.S. Provisional Patent Application Nos. 60/296,114, filed Jun. 7, 2001, 60/296,116, filed Jun. 7, 2001, and 60/297,239, filed Jun. 12, 2001, the disclosures of which are incorporated herein by reference.

BACKGROUND OF THE INVENTION

[0002] 1. Field of the Invention

[0003] The present invention is directed generally to managing use of digital content. In particular, this invention relates to establishing usage rights for controlling such use before the content is created, and distributing licenses to allow use of the content when the content is created.

[0004] 2. Description of Related Art

[0005] One of the most important issues impeding the widespread distribution of digital works via electronic means, and the Internet in particular, is the current lack of protection of intellectual property rights of content owners during the distribution and the usage of the digital content. Efforts to resolve these issues 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.

[0006] Due to the expansion of the Internet in the recent years, and the issues relating to privacy, authentication, authorization, accounting, payment and financial clearing, rights specification, rights verification, rights enforcement, document protection, and collection of licensing fees DRM has become even more important. Because the Internet is such a widely used network whereby many computer users communicate and trade ideas and information, the freedom at which electronically published works are reproduced and distributed is widespread and commonplace.

[0007] Two basic types DRM of schemes have been employed to attempt to solve the document protection problem: 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 IBM's CRYPTOLOPES™ and InterTrust's 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.

[0008] Cryptographic mechanisms are typically used to encrypt (or "encipher") documents that are then distributed and stored publicly, and ultimately privately deciphered by authorized users. This provides a basic form of protection during document delivery from a document distributor to an intended user over a public network, as well as during document storage on an insecure medium.

[0009] 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 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 PCs 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.

[0010] U.S. Pat. Nos. 5,530,235, 5,634,012, 5,715,403, 5,638,443, and 5,629,980 introduced many basic concepts of DRM. The disclosures of all of these patents are hereby incorporated herein by reference in their entirety. For example, U.S. Pat. No. 5,634,012 discloses a system for controlling the distribution of digital works. Each rendering device has a repository associated therewith. A predetermined set of usage transaction steps define a protocol used by the repositories for carrying out usage rights associated with the content. Usage rights are encapsulated with the content or otherwise associated with the digital content to travel with the content. The usage rights can permit various types of use such as, viewing only, use once, distribution, and the like. Rights can be granted based on payment or other conditions.

[0011] In conventional DRM techniques, a content owner, or other authorized party, specifies the rights after the content has been created and protects, e.g. encrypts, the content at the same time. A private key is used to encrypt the content, and a label is generated which specifies the usage rights. The rights label and the protected content are then associated and stored. A license to the content can later be generated for a user to permit the user to use or access the content. The license can include a private key which has been encrypted using a public key in known manner.

[0012] To access the content, the private key can be used to decrypt the encrypted public key, allowing the user to decrypt the content. This technique works well if the content is available at the time of the rights specification. However, this technique breaks-down if one wants to specify rights for content and issue a license for the content before the content is available. For example, a distributor of streaming video to a live future event, or of photographs to a future event, may want to begin selling licenses to the content prior to the event. Conventional DRM systems fall short of presenting processes for improving the security for works that are not yet in existence.

SUMMARY OF THE INVENTION

[0013] A first aspect of the invention is a rights management system for managing use of content having usage rights associated therewith. The system comprises a point of capture system adapted to generate content of a future event when the event occurs. The system also comprises a content distributor adapted to generate a rights label having usage rights associated with content of the future event before the content is generated by the point of capture system, the rights label having a securing mechanism that secures the content when the content is generated. The system further comprises a license server adapted to store the rights label and to issue a license associated with the content from the rights label before the content is generated, the license including a mechanism for unlocking the securing mechanism, and where the content distributor is further adapted to distribute the license before the content is generated.

[0014] A second aspect of the invention is a method for managing use of content having usage rights associated therewith. The method comprises the step of generating a rights label having usage rights associated with content of a future event before the content is generated by a point of capture system, the rights label having a securing mechanism for securing the content. The method also comprises the step of issuing a license associated with the content based on the rights label before the content is generated by the point of capture system, the license including a mechanism for unlocking the securing mechanism. The method further comprises the step of distributing the license before the content is generated.

BRIEF DESCRIPTION OF THE DRAWINGS

[0015] FIG. **1** is a schematic illustration of a DRM system;

[0016] FIG. **2** is a schematic illustration of a rights label;

[0017] FIG. **3** is a schematic illustration of a license;

[0018] FIG. **4** is a flowchart of a method for providing usage rights for digital content before creation of the content in accordance with an embodiment of the invention;

[0019] FIG. **5** is a content creation device for providing usage rights for digital content to be created in the future in accordance with an embodiment of the invention;

[0020] FIG. **6** is a schematic illustration of a conventional streaming media system;

[0021] FIG. **7** is a schematic illustration of a DRM enabled streaming media system in accordance with one embodiment of the present invention;

[0022] FIG. **8** is a schematic illustration of how the DRM system in accordance with one embodiment of the present invention is used to distribute a live event;

[0023] FIG. **9** is a schematic illustration showing the generation of a distribution license in accordance with one embodiment of the present invention;

[0024] FIG. **10** is a schematic illustration showing the generation of a consumer license in accordance with one embodiment of the present invention; and

[0025] FIG. **11** is a schematic illustration showing the generation of a distribution key in accordance with one embodiment of the present invention.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

[0026] The phrase "digital work" as used herein refers to any type of element having content in computer readable form. "Content" as used herein refers to the viewable or otherwise usable portion of a digital work. The phrase "usage rights" refers to manners of use which define permissions granted to a user of an existing digital work or a digital work to be created in the future with respect to use, access, distribution, and the like of the content of the work. In addition, one or more conditions may be specified which must be satisfied before the manners of use may be exercised.

[0027] A DRM system can be utilized to specify and enforce usage rights for items, such as digital content, goods or services. FIG. **1** illustrates a DRM system **10** that can be used to distribute digital content. DRM system **10** includes a user activation device, 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. Typically, when a user goes through an activation process, some information is exchanged between activation server **20** and client environment **30**, and software application **60** is downloaded and installed in client environment **30**. Software application **60** serves as a security component and 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 content **42**.

[0028] 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. License Server **50** manages the encryption keys and issues licenses **52** for exercise of usage rights in the manner set forth below. Licenses **52** embody the actual granting of usage rights to an end user based on usage rights selected from rights label **40**. For example, rights label **40** may include usage rights for viewing protected **42** upon payment of a fee of five dollars and viewing or printing protected content **42** upon payment of a fee of ten dollars. Software application **60** interprets and enforces the usage rights that have been specified in license **52**.

[0029] FIG. **2** illustrates rights label **40** in accordance with one embodiment. Rights label **40** includes plural rights offers **44**. Each rights offer **44** includes usage rights **44***a*, conditions **44***b*, and content specification **44***c*. Content specification **44***c* can include any mechanism for referencing, calling, locating, or otherwise specifying protected content **42** associated with rights offer **44**.

[0030] FIG. **3** illustrates license **52** in accordance with one embodiment. License **52** includes a unique license ID **52***a* and grant **52***b* including usage rights, a principal, conditions, state variables, and a content specification designating an associated protected content **42**. License **52** also includes digital signature **52***c* including any cryptographic keys or the like for unlocking protected content **42**.

[0031] Usage rights specify manners of use. For example, a manner of use can include the ability to use protected content **42**, in a specified way, such as printing viewing, distributing, or the like. Rights can also be bundled. Further, usage rights can specify transfer rights, such as distribution rights, or other derived rights. Such usage rights are referred to as "meta-rights". Meta-rights are the rights that one has to manipulate, modify, and/or derive other usage rights. Meta-rights can be thought of as usage rights to usage rights. Meta-rights can include rights to offer, grant, obtain, transfer, delegate, track, surrender, exchange, and revoke usage rights to/from others. Meta-rights can include the rights to modify any of the conditions associated with other rights. For example, a meta-right

may be the right to extend or reduce the scope of a particular right. A meta-right may also be the right to extend or reduce the validation period of a right.

[0032] As noted above, 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. Usage rights and conditions can exist as separate entities or can be combined. Rights and conditions can be associated with any item including, objects, classes, categories, and services, for which use, access, distribution, or execution is to be controlled, restricted, recorded, metered, charged, or monitored in some fashion to thereby define a property right.

[0033] Protected content **42** can be prepared with document preparation application **72** installed on computer **70** associated with a content distributor, 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 human readable or computer readable content specifying an item, a text file, a code, a document, an audio file, a video file, a digital multimedia file, or any other content.

[0034] 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 some user/machine specific information) being downloaded to client environment **30** in the form of client software application **60** in a known manner. This activation process can be accomplished at any time prior to the issuing of a license.

[0035] When a user wishes to obtain a specific protected content **42**, the user makes a request for 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 protected content **42**. The user can examine rights offers 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** causing both protected content **42** and license **52** to be downloaded. License **52** includes the selected usage rights and can be downloaded from license server **50** or an associated device. Protected content **42** can be downloaded from a computer associated with vendor **80**, a distributor, or another party.

[0036] Application **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.

[0037] DRM system **10** addresses security aspects of protected content **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. Whereas DRM system **10** effectively addresses security aspects of protected content **42**, the system is operable only when protected content **42** is in existence. DRM system **10** cannot readily provide protection to content that is not yet in existence, such as a video stream for a future event.

[0038] FIG. **4** illustrates an embodiment of a method for providing usage rights for content of a digital work before the content is created. In step **100** a rights label specifying usage rights, to be associated with digital content that is not yet created, is generated. The rights label can include plural rights offers each specifying usage rights, such as the right to print, copy, alter, edit or view the digital work or any other right, permission, or restriction, such as those contained in the XrML™ language or other usage rights grammar. In the case of using the XrML™ language, the rights label can be an extensible markup language (XML) document specifying the usage rights. In addition, the future content can have many different versions of usage rights and thus a label can be generated for each version. In step **110**, a key, such as a conventional public key, is generated in a known manner and associated with the rights label.

[0039] In step **120**, a user request for a license to use the content to be created is received. The request can include a selection of one of the offers in the rights label. Keep in mind that the content itself need not be in existence yet. For example, the content can be a video recording or stream of a sporting event to occur in the future. In step **130**, a distributor of the content, or another authorized party, issues a license to the user. The license can include a private key corresponding to the public key generated in step **110** and may include usage rights or other descriptive data. Once again, keep in mind that the content itself need not be in existence yet. Accordingly, the distributor is able to sell a license to view the event prior to the event.

[0040] In step **140**, the content is created. Of course, this step can be accomplished by another party. However the content is created, the salient point in the preferred embodiment is that the content somehow comes into existence after rights are assigned for it. After the content is created, the license is associated with the content in step **150**. The license

can be encapsulated with the content. Alternatively, the license can be stored separately from the content but be associated through links, flags, calls, references or the like. Therefore, the term "associated" as used herein refers broadly to creating a correspondence between the content and the license so the license will be applied to the content. Once the license is associated with the content, the content is secured using the key generated in step **110**. The digital content can be secured through any form of encryption or other known technique. For example pretty good privacy (PGP) encryption procedures can be used.

[0041] In step **160**, the process determines whether there is a request for access to the secured digital content. If there are no requests, the process waits for a request. However, if there is a request for access, the process proceeds to step **170** where the usage rights associated with the digital work, i.e. usage rights in the license, are checked to determine whether all the conditions, such as payment, associated with the usage rights have been satisfied. If all the conditions have been satisfied, the process proceeds to step **180** in which access to the content is granted, i.e., the content is downloaded, streamed, or otherwise made accessible to the user. In step **190**, the user's private key is used to decrypt the content in a known manner.

[0042] The association of the usage rights with the content may occur in a variety of ways. For example, if the usage rights will be the same for the entire content of a digital work, the usage rights can be attached when the digital work is processed for deposit in a distribution server or other device. However, if the content of the digital work has a variety of different usage rights for various components, the usage rights can be attached as the work is being created. Various authoring tools and/or digital work assembling tools can be utilized for providing an automated process of attaching the usage rights. Because each part of a digital work can have its own usage rights, there can be instances where the usage rights of a "part" will be different from its parent. As such, conflict rules can be established to dictate when and how a right may be exercised in a known manner.

[0043] FIG. **5** illustrates a content creation device, a video recorder, in accordance with one aspect of the present invention. The content creation device **300** includes a controller **302**, a LCD display **304**, a smart-card reader **306**, a memory **307**, a keypad **308**, a rights assignment engine **310**, eye/iris recognition sensors **312**, a cable connection **313**, a handle **314**, and symmetric finger print recognition sensors **316**,**318**. Also, lens system **320** permits recording of video images. Controller **302** and rights assignment engine **310** of the illustrated embodiment are accomplished through a microprocessor based device programmed in a desired manner.

[0044] While FIG. **5** shows the controller **302** and the rights assignment engine **310** as separate units, the functions performed by these units may be combined in one processor or may be further divided among plural processors such as digital signal processors and/or performed by dedicated hardware such as application specific integrated circuits (ASIC), e.g., hard-wired electronic or logic circuits or programmable logic devices, or other hardware or software implementations.

[0045] The smart-card reader **306** can be used for reading cards inserted therein. For example, a license or identification can be embedded in the card and communicated to the controller **302** and/or the rights assignment engine **310**. LCD display **304**, the smart card reader **306**, keypad **308** and software interfaces constitute a user interface of creation device **300**. The user interface permits a user to input information such as identification data, and access requests and provides feedback as to operation of creation device **300**. The content creation device **300** of the preferred embodiment is a video recorder, however, it can be any type of recording device, or content creation device for example, a still-image camera, an animation generator, an audio recorder, a text processor, or the like.

[0046] The rights assignment engine **310** can be accessed via the cable connection **313**. For example, a rights assignment computer of a digital rights management (DRM) system, as described in further detail below, can be coupled to the rights assignment engine **310** via cable connection **313** to download a usage rights label or template, similar to the label described above, indicating usage rights for content to be created by the content creation device **300** in the future. Any content created by the content creation device **300** will automatically be associated with the usage rights label or labels stored in rights assignment engine **310**. Alternatively, the usage rights label can be composed using the user interface of creation device **300**. In either case, one or more labels and corresponding keys generated and stored in rights assignment engine **310** along with instructions indicating how the labels are to be assigned to content created by creation device **300**.

[0047] The instructions can cause the usage rights labels to be assigned in any manner and can include any permissions and/or restrictions. For example, in the case of a video recorder, each part of the video sequence or frames can selectively be assigned different rights. This makes the rights assignment process very flexible and dynamic and permits rights assignment to be made in real time as content is created or prior to creation.

[0048] The content creation device **300** can utilize a unique device ID, a user's smart card, PKI technology, a PIN, or any biometrics system to assign rights based on the identity of the user, the recording device itself, the data on the smart card, or the like. For example, fingerprint recognition sensors **316**, **318** or iris recognition sensor **312** can be used for recognition or authentication of the user's identify to permit rights assignment engine **310** to use a corresponding set of rights associated with the user. For example, all content recorded by person A will have one set of rights and all content recorded by person B will have a different set of rights. Of course, all these features, for example, fingerprint recognition sensors **316**, **318** or iris recognition sensor **312**, are optional features and content creation device **300** may be operated in a more conventional manner in other embodiments.

[0049] The content creation device **300** records content in a conventional manner. However, labels and keys generated in steps **100** and **110** described above are stored and associated with content recorded by content recorder **300** during or soon after recording. Accordingly, steps **140** and **150** described above are also accomplished by content creation device **300**. For security purposes, a token or pre-paid card (or magnetic card and smart card, or any of its variations, such as memory-type or synchronous communication card, ISO 7816-compliant card, EMV-type card) can be used for the storage of fees and micro-payments, or keeping track of those fees with associated rights. Such cards can be read using the smart card reader **306**. Again, however, these features are optional features and content creation device **300** may be operated in a more conventional manner in other embodiments.

[0050] It can be seen that the invention permits usage rights for a work to be created and associated with content prior to the creation of the content, the usage rights defining how the

future digital work may be used and distributed. These pre-established usage rights become part of the future digital work and control the manner of use of the content of such work.

[0051] In the preferred embodiment, after the rights have been established for future content, a private key associated with the future content is assigned and a rights label is generated. This private key, along with the rights label, is stored. A user can purchase the content (present or future) after the label has been inserted into the main server. After the content is purchased, the content owner can get a license for encryption which contains the public key encrypted by a private key. Alternatively, a single symmetric key can be used.

[0052] The preferred embodiment allows a newspaper editor, for example, to send a camera crew to record content without worrying about the pictures being compromised in any way (for example, altered, edited, viewed by unauthorized personnel, or hidden and separately sold to another newspaper organization). In fact, the camera crew may have no rights whatsoever in the content as soon as the content is recorded.

[0053] Alternatively the editor can set the rights in such a way that the first **10** pictures, for example, will belong to the newspaper (work-related), and the next five pictures will belong to the cameraman (for personal use). This example illustrates the flexibility, security, confidence, certainty, and multiple relationships that can be arranged between parties (the cameraman and the editor in this example).

[0054] All future content may be assigned a content ID prior to existence of the content. Given the content ID information and the license for encryption, the content can be encrypted after creation in a manner that is available to be used by the users who have purchased the license. However, if the content ID information and the license for encryption are not available, access to the content shall be denied.

[0055] Further, a predetermined symmetric key can be generated in advance of content creation, and stored with the rights label. Afterwards, the same key can be used to encrypt the content once it is created. However, as noted above every user can receive a different key. In another alternative, the user can be given an authorization token, which the user can exchange for the license later on.

[0056] The controller **302** can process the security parameters and the rights management steps. Lost-card verification, lost-card reports, card-usage reports, security alert reports, and tracking reports can be associated or combined with the rights management reports, such as reports for revoked rights, denied rights, renewed rights, usage patterns, and micropayments.

[0057] The distribution, accounting, and other functions of the distributor and clearinghouse can be accomplished by any party on any device. For example, the content can be rendered on an ebook reader or PDA in response to entry of a code or insertion of a smartcard into a reader and accounting can be accomplished when the digital work or accounting data is returned to a specific source. The division of tasks disclosed herein is only an example. Usage rights and or accounting data can be encapsulated with the digital work or can be stored separately. Code for rendering, decrypting, or otherwise permitting or limiting use of the content can be stored on any device or can be encapsulated with the digital work. Any distribution arrangement can be used with the invention and such arrangements can include any combination of devices, such as personal computers, servers, PDAs, and the like communicating with one another in any manner as is necessary to transfer the desired information.

[0058] FIG. **6** is a schematic illustration of a streaming media system **400** for streaming an event **402**, such as a soccer match shown, or any other event. The media system **400** includes a capturing device which in the illustrated example, is a video camera **404** that captures event **402** and provides a video stream thereof. The video stream from the video camera **404** is received by an encoder device such as a video stream encoder **406** that converts the video stream into a streaming format such as Quicktime™, Real Media™ or Windows Media Player™. The converted video stream is provided to a streaming server **408** that serves the content via a network such as the Internet **410** to end users **412**. The content is then viewed by the end users **412** using rendering application(s) that displays the video content on a display device **414**. However, the streaming media system **400** does not allow protected distribution of the event **402** since a license is not required to view the event **402**. Correspondingly, the streaming media system **400** also does not allow distribution of protected content. In addition, streaming media system **400** does not allow distribution of protected content if the content does not yet exist, such as is the case where the event is to occur in the future.

[0059] Therefore, in accordance with one embodiment of the present invention, DRM-enabled streaming media system **500** is provided as shown in FIG. **7** where the streaming media, for instance, a video stream, is protected, and a license is required to view or access the content thereby allowing protected distribution of the content. It should be initially noted that whereas the terms "server" and "system" are used herein 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 for executing the described function, such as a personal computer, hand held computer, PDA, or any other general purpose programmable computer or combination of such devices, such as a network of computers. In addition, as previously noted, "content" can be a human readable or computer readable content, a text file, a code, a document, an audio file, a video file, a digital multimedia file, or any other content.

[0060] In the DRM-enabled streaming media system **500**, the event is captured by the capturing device **504**, thereby providing the content to be protected. The capturing device **504** may be a video camera of the type previously described relative to FIG. **5** or **6**. The capturing device **504** provides captured video stream to a content preparation device **508** and a video stream encoder **506**. The video stream encoder **506** is preferably integrated with the content preparation device **508** as shown.

[0061] The DRM content preparation device **508** which may be similar to the rights assignment engine **310** described relative to FIG. **5**, generates a rights label **510** associated with the content to be created. The rights label **510** includes various rights associated with particular content, conditions that must be satisfied to access the content, and a content encryption key needed to decrypt the content. The rights label **510** is stored in a database **512** controlled by a license server **514**. The license server **514** is adapted to issue licenses **532** based on offers selected from the rights label **510** for allowing use of protected content in the manner described further below. In addition, a video stream encoder **506** encrypts the content so that it becomes encrypted content **505** which is protected in the sense that content must be decrypted in order to use the

content. Preferably, the video format is preserved even through encryption. The encrypted content **505** is provided to a video stream server **516** that hosts the encrypted streamed content. The video stream server **516** provides the encrypted content **505** to a network such as the Internet **520** to allow distribution to remote users **522**.

[0062] Rendering devices **526** can, upon activation by an activation device such as the activation server **533**, process the licenses **532** issued by the license server **514**. The rendering application **524** is preferably integrated with the rendering devices **526** used by the users **522**. The rendering application(s) **524** may be Quicktime™, Real Media™ or Windows Media Player™ that allow display of video content on rendering device **526**, or other appropriate rendering application.

[0063] The activation server **533** is preferably used to generate public-private key pairs for the users **522** of the DRM system **500**. Activation provides a means for authenticating the users **522** via presentation of an issued public key provided during the activation process. During the generation of the licenses **532**, the public key of the users **522** received during the activation process are retrieved. The content encryption key provided in the rights label **510** is then encrypted using the user's public key and delivered in the licenses **532**. The only way to decrypt the content encryption key provided in the rights label **510** is by using the user's private key received during the activation process. Furthermore, the only way to decrypt the encrypted content is to use the decrypted content encryption key received in the rights label **510**. When a user **522** attempts to view or play a video stream, a license **532** is issued by the license server **514** and sent to the DRM component **530** of the user **522**. The license **532** contains the rights and content encryption key that may be decrypted using the user's private key to allow decryption of the encrypted content **505**. Once the encrypted content **505** is decrypted, normal viewing of the content is attained using the rendering application **524**. Thus, by encrypting the content as well as the encryption key required to decrypt the content, the DRM system **500** ensures that only authorized users are given access to the protected content.

[0064] Of course, depending on the specific implementation of the DRM system, other parties involved in the implementation of the DRM system **500** in addition to users **522** that actually consume content, may also need to be activated. For example, a point of capture that produces the content, content distributor, vendor such as a store front or an application that allows purchase and streaming of the content, may also need to be activated depending on the specific implementation in accordance with other embodiments.

[0065] Although the DRM system **500** shown in FIG. **7** discussed above can be used to support and distribute any type of protected content, the DRM system **500** shown, does not provide for assignment of rights to content that does not yet exist. Moreover, the DRM system **500** also does not provide for pre-distributing of licenses granting rights to view content before the existence of the content. Alternative embodiments of the DRM systems in accordance with the present invention discussed below address this limitation.

[0066] In particular, the preferred embodiment of a DRM system **600** in accordance with the present invention as schematically shown in FIG. **8** establishes a distributor license **620** with a distribution key **624** discussed in detail below to allow protection of content that does not yet exist such as a broadcast of a future live event, and also to allow the distribution of licenses in advance of the event. As seen in FIG. **8**, a live event **602** is captured by capturing device such as a video camera **604**, and captured video data is provided to a streaming device such as a streaming server **616**. In accordance with the present embodiment, the streaming server **616** is authorized via a distributor license **620** to distribute the captured video stream as encrypted content **605** to users **612** via the Internet **610**. The encrypted content **605** is decrypted by users **612** using consumer licenses **630** and video content is displayed on rendering devices **626** using a rendering application such as Quicktime™, Real Media™ or Windows Media Player™. It should be noted that in FIG. **8**, various components of the DRM system **600** such as a content preparation device, video stream encoder, license server and activation server have been omitted for clarity. However, such components would function in a substantially similar manner as described relative to DRM system **500** of FIG. **7** discussed above.

[0067] As shown in FIG. **8**, the distributor license **620** of the illustrated embodiment comprises a distribution key **624**, distributor rights **625**, and stream metadata **627**. In a similar manner, the consumer license **630** of the illustrated embodiment comprises a distribution key **634**, consumer rights **635**, and content metadata **637**. The distribution key **624** is a content encryption key that is generated in advance of the event, and is associated with the rights and conditions that will apply to the future broadcasted content. The distribution key **624** is stored as a component of a rights label in a license server as discussed in further detail relative to FIGS. **9** to **11** below. As will be evident to one of ordinary skill in the art in view of the teachings presented below, the distributor license **620** and the consumer license **632** are generated and issued to authorized end users prior to, or even during, the live event.

[0068] FIG. **9** is a schematic illustration showing the generation and retrieval of the distributor license **620** of FIG. **8** in accordance with one embodiment of the present invention. As previously noted, the distributor license **620** can exist prior to the event to protect captured event content through encryption, and to distribute the protected content to the users **612**. A content distributor **702** owns rights to the captured content, and in the present example, may be a broadcaster or the entity that owns the copyright for the broadcast. A point of capture system **704** is a system used to capture the event and prepare the content for distribution through a streaming device such as streaming server **616** discussed above. Point of capture system **704** may comprise a capturing device such as the video camera **504**, the content preparation device **508**, and/or the video stream encoder **506** discussed previously relative to FIG. **7**. These components have been omitted in FIG. **9**. Of course, in other embodiments, alternative appropriate devices may also be used.

[0069] It should also be noted that the point of capture system **704** which captures the event can be directly associated with the content distributor **702** as shown in FIG. **9**, for instance, where the content distributor **702** controls or owns the point of capture system **704**. However, in other embodiments, the point of capture system **704** may be a separate entity not associated with the content distributor **702**.

[0070] A vendor **730** runs a web site, such as an on-line store front, where access to the event is sold and/or otherwise obtained by users. After some transaction by an end user such as log-in, payment, etc., a request to use protected content associated with a future event is made. The content distributor **702**, the vendor **730** or equivalent, requests issuance of an

appropriate distribution license **620** associated with the requested future event to the license server **740**.

[0071] The license server **740** is provided with a public key **744** from the point of capture system **704**, and is responsible for issuing both the consumer license **630** and the distribution license **620** from the rights label **750** stored in the license server **740**. The rights label **750** includes metadata **752**, distributor rights **625**, consumer rights **635**, and the distribution key **624** as shown. In a manner similar to that previously described, the distribution key **624** itself is encrypted using the public key **744** from the point of capture system **704**. Thus, the distribution key **624** itself, must be decrypted so that the distribution key **624** can be used to decrypt protected content. Further details regarding generation of the distribution key **624** is discussed relative to FIG. **11**. Metadata **752** is included in the rights label **750** that may be used for authentication purposes. The distributor rights **625** may include meta-rights such as rights to offer, grant, obtain, transfer, delegate, track, surrender, exchange, and revoke usage rights to/from others. Meta-rights can also include the rights to modify any of the conditions associated with other rights. For example, a meta-right may be the right to extend or reduce the scope of a particular right or the validation period of a right.

[0072] As shown, the distribution key **624** and the distributor rights **625** of the rights label **750** are used to generate the distributor license **620**, the distributor license **620** being completed by inclusion of a stream metadata **627**. In the present example, the distributor license **620** is provided to the content distributor **706** to allow distribution of the content, and to point of capture system **704** to allow encryption of the content. In this regard, the distribution license **620**, and in particular, the distribution key **624** in the generated distribution license **620**, is used to encrypt the captured event by the point of capture system **704**, for instance, video or audio stream of the event.

[0073] The actual locale where the protection occurs depends on the implementation of the point of capture system **704**. In the example where the DRM system in accordance with the present invention is used to encrypt a video stream, the encryption of the video stream may occur anywhere along the stream creation workflow prior to distribution via the Internet **610** of FIG. **8**, or other distribution channel. Additional security measures such as protection of the video data from the capturing device **604** to the streaming server **616** may also be provided.

[0074] FIG. **8** illustrates generation of the consumer license **630** shown in FIG. **8** in accordance with one embodiment of the present invention, the consumer license **630** being required for users to use the protected content such as to view video stream of an event. Typically, in implementing a DRM-enabled distribution system in accordance with the present invention, an end user **612** seeking to purchase protected content accesses the vendor **730**, which may be an on-line storefront or a web site. As previously noted, the vendor **730** provides the access point for consumers such as end users **612** to purchase content which is not yet available, but will be available at a predetermined date, for instance, a future event.

[0075] When attempt is made by the end user **612** to purchase protected content, the public key **613** of the end user **612** which was previously obtained through an activation process, is sent to the license server **740**. The license server **740** uses the public key **613** to encrypt the distribution key **624** required to decrypt the protected content, and generates the consumer license **630** using components of the rights label **750**. In particular, the consumer rights **635** and the distribution key **624** are used to generate the consumer license **630**, the consumer license **630** being completed by inclusion of the metadata **754** that may be used for authentication purposes. The license **630** can then be downloaded by the end user **612** and used for accessing the scheduled future event.

[0076] The above described process for obtaining a consumer license **630** by the end user **612** is somewhat similar to conventional DRM systems. However, in contrast to conventional DRM systems, the obtained consumer license **630** cannot be used for any present content, but instead, serves as a "ticket" for a future event which may be a live event. The consumer license **630** is generated in accordance with the consumer rights **635** that have been specified to the end user **612**. Thus, in the manner described above, the license server **740** of the preferred embodiment makes a distinction between the rights specified for the distributor and the rights specified for the consumer to generate a distributor license **620** or a consumer license **630** accordingly.

[0077] FIG. **11** is a schematic illustration showing the generation of the distribution key **624** that is a component of the rights label **750** in accordance with one embodiment of the present invention. The distribution key **624** is required for generating the distribution license **620** and the consumer license **630** which are necessary for distributing and allowing use of protected content that is to occur in the future, such as a future event. Through a software application, the content distributor **702** initially creates the distribution key **624**, which is a symmetric encryption key. The distribution key **624** is protected from tampering by encrypting it with the license server's **740** public key **742** so that only the license server **740** will be able to decrypt the distribution key **624**. In this regard, the distribution key **624** is preferably stored in the license server **740** in order to provide better security and to track its use.

[0078] Moreover, as previously noted, additional metadata **752** is created and stored in the rights label **750**. This metadata **752** is later inserted into the header information of the video stream that is generated by the point of capture system **704** during the live event. This metadata **752** may be used by the end users **612** to authenticate the issued licenses. The rights label **750** is transferred and stored in the license server **740** and may also be updated therein. The distribution key **624** is then issued as a component of the distributor license **620** and/or the consumer license **630** to a distributor and/or end user **612**, respectively, in the manner described relative to FIGS. **9** and **10**. The above described process is somewhat similar to processes used in conventional DRM systems except that the distribution key **624** is not immediately used to protect or use content, but it is saved for later use when the protected content is to be distributed closer to the time of the actual future event.

[0079] The following describes an example workflow that may be used to operate a DRM system in accordance with one embodiment of the present invention as applied to protected distribution and viewing of a future event. Thus, FIGS. **7** to **11** and various components identified therein should be referenced to facilitate understanding of the workflow. Initially, the content distributor **702** decides to offer a future event for sale, for instance, a future sporting event. The content distributor **702** creates the distribution key **624** which is a symmetric encryption key. The distribution key **624**, together with additional information including distributor rights **625** and metadata **752** is encoded in rights label **750**. The rights label

750 is then transferred to the license server **740** at which the consumer rights **635** is also added to the rights label **750**.

[0080] The vendor **730** which may be a storefront or a web site, offers for sale the right to view the future event. End user(s) **612** desiring to use or otherwise view the future event, accesses the vendor **730** via the Internet **610** to purchase, or otherwise obtain, the right to view the future event. During the purchasing transaction, the vendor **730** interacts with the license server **740** to generate the consumer license **630** in the manner described above relative to FIG. **10** from rights label **750** so that the end user **612** can download the consumer license **630** to the user's **612** rendering device **626** or any other appropriate device such as a computer, hand held device, etc. for future use in viewing the event.

[0081] During this time when the right to view the future event is offered for sale via the vendor **730**, but prior to the start of the actual event, the content distributor **702** requests for the distributor license **620**, which is issued by the license server **740** in the manner described above relative to FIG. **9**. The distributor license **620** is then used by the point of capture system **704** to protect the content while capturing the live performance of the event, for instance, the sporting event **602**. The point of capture system **704** processes the video data from the capturing device **604** on-the-fly, and transmits now protected content **605** to the streaming server **616**.

[0082] Once the distribution license **620** and the consumer license **630** are issued, the event can be securely distributed and consumed by authorized audience, i.e. end users **612**. The streaming server **616** provides now protected content **605** through the Internet **610**, or other appropriate distribution mechanism, to every user **612** that has purchased the right to view the event. User **612** decrypts the encrypted distribution key **624** provided in the consumer license **630** to decrypt the protected content **605**. User's **612** rendering device **626** (FIG. **8**) includes a rendering application such as Quicktime™, Real Media™ or Windows Media Player™ so that user **612** can view the event.

[0083] The preferred embodiment as described above can be used in a subscription model (for example, for magazine or marketing reports) in which the future issues of the content have not been published, but the rights for those issues have already been assigned and stored. At an appropriate future time, the rights will be associated with the corresponding content. By selling the content of a future event through a vendor such as a web site before the actual event, the traffic of the web site or other distribution device can be drastically reduced and distributed over a longer period of time, making the requirements for the servers and the web site easier to satisfy and less expensive to operate. Note, however, that the entity selling the rights or tickets, i.e. the license, might be different from the entity providing the content later on.

[0084] It should again be understood that whereas the terms "server" and "system" are is 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 for executing the described function, such as a personal computer, hand held computer, PDA, or any other general purpose programmable computer or combination of such devices, such as a network of computers. 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 devices and components 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, the software package and/or licenses 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 include any mechanism for enforcing security and need not include a rendering application or the like.

[0085] 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 grammar such as XrML™ can be used. In addition, software using objects or an object-oriented software development environment may be used that provides portable source code that can be used on a variety of computer hardware platforms. For example, the software used in implementation of the present invention can be written in the JAVA™ language and run in a JAVA™ virtual machine. Alternatively, the disclosed operations may be implemented partially or fully in a hardware using standard logic circuits or VLSI designs. The hardware can include any type of general purpose computer, dedicated computer, or other devices.

[0086] 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 within the scope of the appended claims and legal equivalents.

We claim:

1. A computer-implemented method executed by one or more computing devices for controlling use of future content, the method comprising:

selecting, by at least one of the one or more computing devices before the future content is available, a usage right included in at least one rights offer associated with the future content;

requesting, by at least one of the one or more computing devices before the future content is available, generation of an authorization token associated with the future content;

transmitting, by at least one of the one or more computing devices, device information and information identifying the authorization token;

receiving, by at least one of the one or more computing devices, an indication that the future content is available; and

receiving, by at least one of the one or more computing devices, a data stream representing the future content.

2. An apparatus for controlling use of future content, the future content being a recorded representation of a future event, the 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:

select, before the future content is available, a usage right included in at least one rights offer associated with the future content;

request, before the future content is available, generation of an authorization token associated with the future content;

enable the transmission of device information and information identifying the authorization token;

enable the receipt of an indication that the future content is available; and

enable the receipt of a data stream representing the future content.

3. At least one non-transitory computer-readable medium storing computer-readable instructions that, when executed by one or more computing devices, cause at least one of the one or more computing devices to:

select, before the future content is available, a usage right included in at least one rights offer associated with the future content;

request, before the future content is available, generation of an authorization token associated with the future content;

transmit device information and information identifying the authorization token;

receive an indication that the future content is available; and

receive a data stream representing the future content.

* * * * *