Office de la Propriété Intellectuelle du Canada
Un organisme d'Industrie Canada

Canadian Intellectual Property Office
An agency of Industry Canada

CA 2432189 A1 2002/12/19

(21) 2 432 189

(12) DEMANDE DE BREVET CANADIEN
CANADIAN PATENT APPLICATION

(13) A1

(86) Date de dépôt PCT/PCT Filing Date: 2002/06/05
(87) Date publication PCT/PCT Publication Date: 2002/12/19
(85) Entrée phase nationale/National Entry: 2003/06/17
(86) N° demande PCT/PCT Application No.: US 2002/017610
(87) N° publication PCT/PCT Publication No.: 2002/101490
(30) Priorité/Priority: 2001/06/07 (60/296,115) US

(51) Cl.Int.^{7}/Int.Cl.^{7} G06F 19/00

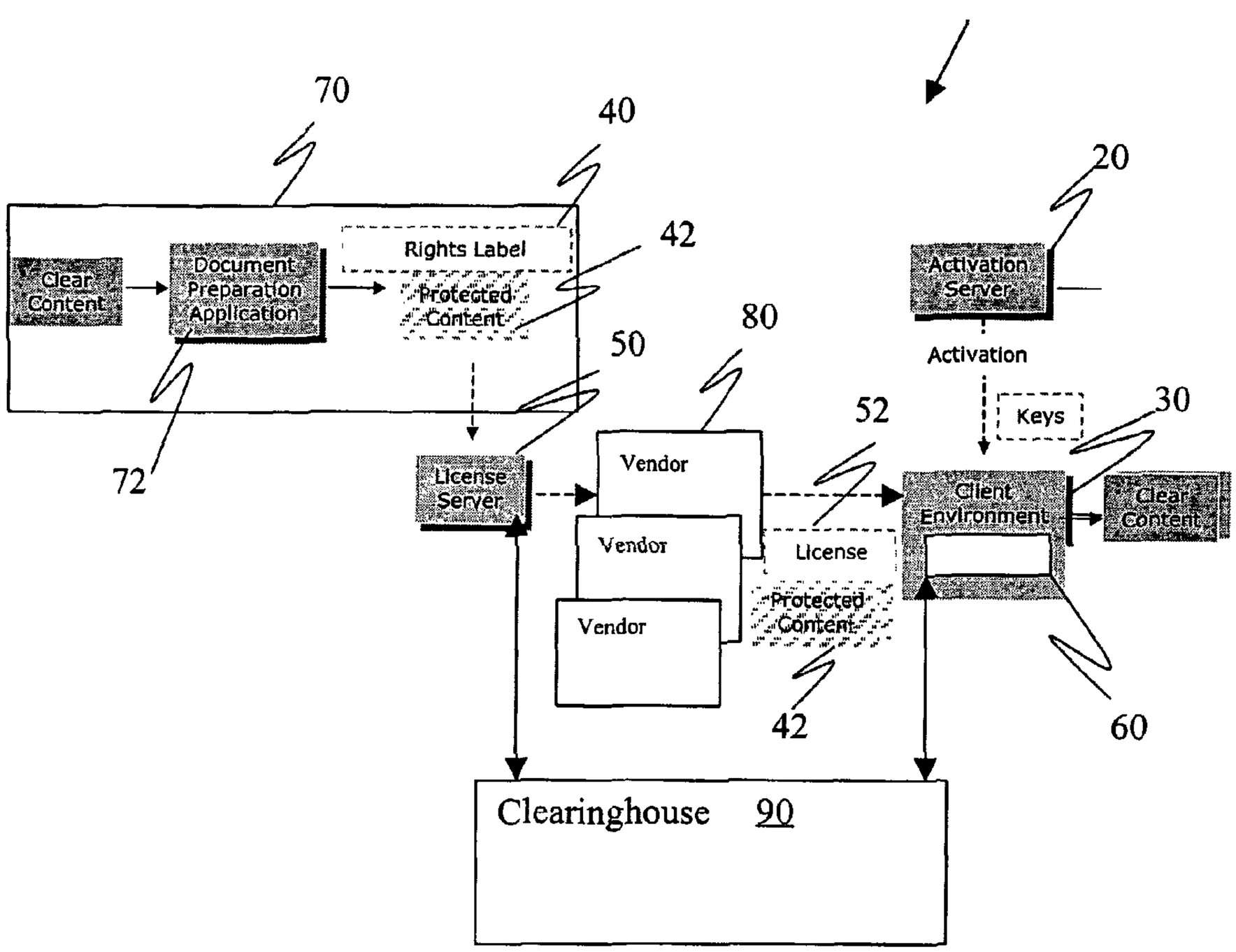
(71) Demandeur/Applicant:
CONTENTGUARD HOLDINGS, INC., US

(72) Inventeurs/Inventors:
LAO, GUILLERMO, US;
WANG, XIN, US;
TA, THANH, US;
FUNG, JOSEPH Z., US

(74) Agent: ROBIC

(54) Titre : PROCEDE ET DISPOSITIF POUR GERER LES ZONES DE CONFIANCE MULTIPLES DANS UN SYSTEME DE GESTION DES DROITS D'AUTEUR ELECTRONIQUES

(54) Title: CRYPTOGRAPHIC TRUST ZONES IN DIGITAL RIGHTS MANAGEMENT



(57) Abrégé/Abstract:
Cryptographic keys are used to protect content (42) in a digital rights management system. Activation servers (20) cooperate with license servers (50) to issue licences (52) to user devices (60) associated with differing trust zones.

(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 02/101490 A3

(51) International Patent Classification[7]: G06F 19/00

(21) International Application Number: PCT/US02/17610

(22) International Filing Date: 5 June 2002 (05.06.2002)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/296,115 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) Inventors: **LAO, Guillermo**; 5531 Lorna Street, Torrance, CA 90503 (US). **WANG, Xin**; 3005 Shrine Place, #8, Los Angeles, CA 90007 (US). **TA, Thanh**; 18694 Stratton Lane, Huntington Beach, CA 92648 (US). **FUNG, Joseph, Z.**; 13452 Beach Street, Cerritos, CA 90703 (US).

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

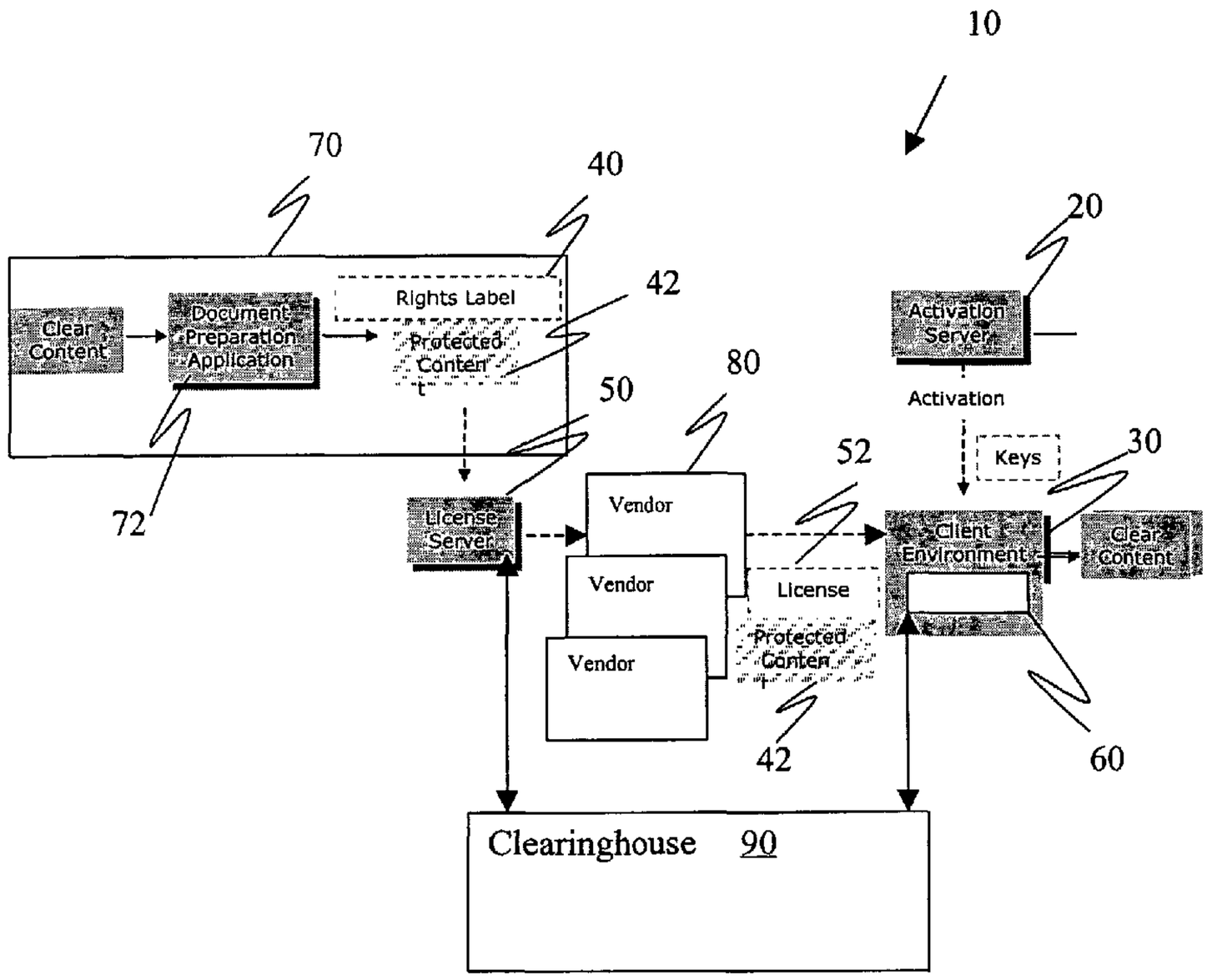
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, 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*
— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

[Continued on next page]

(54) Title: CRYPTOGRAPHIC TRUST ZONES IN DIGITAL RIGHTS MANAGEMENT



(57) Abstract: Cryptographic keys are used to protect content (42) in a digital rights management system. Activation servers (20) cooperate with license servers (50) to issue licences (52) to user devices (60) associated with differing trust zones.

WO 02/101490 A3

WO 02/101490 A3

(88) Date of publication of the international search report:
5 June 2003

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.

METHOD AND APPARATUS FOR SUPPORTING MULTIPLE TRUST ZONES IN A DIGITAL RIGHTS MANAGEMENT SYSTEM

BACKGROUND OF THE INVENTION

Field of the Invention

[0001] The present invention is directed to systems for controlling the distribution of items, such as digital content. In particular, the present invention is directed to such systems that support multiple trust zones.

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 implementations of DRM Systems work well in a single activation server system, where the activation server provides one or more clients with a public and private key pair, or other identification mechanism, during activation to allow the client to access and use the protected content based on provisions specified by a license issued by one or more license servers. The single activation by a single activation server system allows the same activation to be used to enforce usage rights for all the content protected with the DRM System. By allowing the activated client to discern cryptographic signatures, signatures by license servers that have not been activated by the same activation system will be rejected which means that there will be interoperability problems if more than one activation system is provided in the DRM System. However, the multiplicity of parties to electronic transactions and various business models in use today often results in multiple activation systems and the resulting multiplicity of activations for content from various systems. Such multiple activations complicate the user experience because different sets of keys, or other identification mechanism, are required to use different content.

SUMMARY OF THE INVENTION

[0009] A first aspect of the invention is a rights management system for managing use of items having usage rights associated therewith. The system comprises a first activation device defining a trust zone and adapted to issue a first software package that enforces usage rights, a second activation device defining a second trust zone and adapted to issue a second software package that enforces usage rights, and at least one first license device associated with said first trust zone. The first license generates a license associated with the items and including usage rights specifying a manner of use. The license also specifies one or more trust zones in which the license is valid. At least one user device is associated with the first trust zone and

receives the first software package and the license to use the items in accordance with the license.

[0010] A second aspect of the invention is a rights management system for managing use of items having usage rights associated therewith. The system comprises a plurality of activation devices, defining trust zones and being adapted to issue a software package that enforces usage rights to control use of the items, at lease one license device associated with each of the trust zones, the license devices being adapted to generate a license associated with the items and having usage rights specifying a manner of use. The license also includes a designation as one of an open and closed license. A plurality of usage devices are associated with one of the trust zones and receive the software package and the license to use the items in accordance with said license.

[0011] A third aspect of the invention is a rights management system for managing use of items having usage rights associated therewith. The system comprises a first activation device defining a first trust zone, a first license device associated with the first trust zone and adapted to generate an open license having usage rights associated with a first item, a second activation device defining a second trust zone and adapted to issue a software package that enforces usage rights to control use of the first item, and a user device associated with the second trust zone and adapted to receive the software package from the second activation device, and the open license to use the first item in accordance with the open license.

[0012] A fourth aspect of the invention is a method for managing use of items having usage rights associated therewith. The method comprises defining a first trust zone and a second trust zone, each trust zone having an activation device associated therewith and adapted to issue a software package that enforces usage rights to control use of said items, and generating a license associated with the items in the first trust zone, wherein the license includes usage rights specifying a manner of use and a

specification of at least one of an open license and a closed license that determines whether the items are usable in at least one of the first trust zone and the second trust zone.

[0013] A fifth aspect of the invention is a method for enforcing a license. The method comprises granting usage rights associated with a protected item to control use of the protected item within a trust zone, determining whether the license was issued in the trust zone or outside of the first trust zone, and determining whether the license is an open license or a closed license. If the license is a closed license issued outside of the trust zone, use of the protected item within said trust zone is prohibited and if the license is an open license issued outside of the trust zone, use of said protected item within the trust zone is permitted.

[0014] A sixth aspcet of the invention is a license adapted to be associated with a protected item to control use of the protected item. The license comprises usage rights that specify a manner of use for the protected item; and, license classification indicating whether the license is an open license a permitting use of the protected item outside of the trust zone or a closed license prohibiting use of the protected item outside of the trust zone.

BRIEF DESCRIPTION OF THE DRAWING

[0015] The invention is described through a preferred embodiments and the attached drawing in which:

[0016] Fig. 1 is a schematic illustration of a DRM System;

[0017] Fig. 2 is a schematic illustration of a rights label;

[0018] Fig. 3 is a schematic illustration of a DRM system with a plurality of activation servers that each define a trust zone in accordance with one embodiment of the present invention;

[0019] Fig. 4 is a schematic illustration of another DRM system having a top-most activation server in accordance with another embodiment of the present invention;

[0020] Fig. 5 is a schematic illustration of a license in accordance with the preferred embodiment; and

[0021] Fig. 6 illustrates a method of generating licenses in accordance with the preferred embodiment.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

[0022] A DRM system can be utilized to specify and enforce usage rights for specific content or other item. 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 client component 60 is downloaded and installed in client environment 30. Client component 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.

[0023] 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. Client component 60 interprets and enforces the usage rights that have been specified in license 52.

[0024] 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 44c. Content specification 44c can include any mechanism for referencing, calling, locating, or otherwise specifying protected content 42 associated with rights offer 44.

[0025] 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.

[0026] In many 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. 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.

[0027] 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, a text file, a code, a document, an audio file, a video file, a digital multimedia file, or any other content.

[0028] 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.

[0029] 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 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 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.

[0030] Applicant 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.

[0031] 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.

[0032] DRM system 10 shown in Fig. 1 works well in a single activation server implementation, i.e. a system in which one or more devices, such as activation server 20 of Fig. 1, comprise a single activation system.

[0033] Activation by a single activation system is desirable because the same activation process can be used to control use of all protected content 42. However, when client component 60 discerns cryptographic signatures, signatures by license devices other then activation server 20 will be rejected. This means that there will be interoperability problems if more than one activation server system is used. However, the multiplicity of parties and complex business models in use today often result in multiple activation server systems and a multiplicity of activation processes. For example, a user may wish to use items such as protected content from different unrelated sources. In such a case, each source would require a unique activation process. Such multiple activations would complicate the user experience because different sets of keys are required to use different content, even when the content is protected with the same DRM system. On the other hand, it is often desirable to restrict use of content only to parties activated by a specific activation system.

[0034] In accordance with one preferred embodiment of the present invention, trust zones are associated with an activation device. Open licenses allow the protected items, such as digital content, to be used in any trust zone

and closed licenses allow the protected items such as digital content, to be used only within a designated trust zone or plural designated trust zones.

[0035] Fig. 3 illustrates DRM system 200 of the first preferred embodiment which is described in further detail below. Initially, it should be understood that whereas the term “server” and “client” are used below to describe the devices for implementing the present invention in the embodiments 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, or any other general purpose programmable computer, or combination of such devices, such as a network of computers may be used.

[0036] DRM system 200 includes first and second activation devices such as two activation servers 210 and 250 that define trust zones 212 and 252, respectively. It is understood that system 200 can have more than two activation servers and corresponding trust zones. Activation server 210 issues public and private key pairs, or another identification mechanism, to user devices such as clients 216 within the trust zone 212. The key pairs allow clients 216 to use protected content in the manner further described below. In addition, in the present example, license device(s) such as license servers 220 are associated with trust zone 212 and are operative to generate licenses 253 in a known manner. Similarly, activation server 250 provides private and public key pairs to clients 256 to allow use of protected content based on the provisions of a license. License servers 260 are associated with trust zone 252 are operative to generate licenses 253.

[0037] Activation servers 210 and 250 provide unique private and public key pairs as well as other elements in a software package which is downloaded during an activation procedure by the respective clients in trust zones 212 and 252, respectively. The software package may possess information such as identification or user information, and may be adapted to

perform certain functions, for example, rendering and cryptographic functions. The software packages provided to respective clients are used by the clients as a security component to enforce licenses and thus control use of protected content.

[0038] In the preferred embodiment, two different types of licenses 253 are issued by the license servers 220 and 260: an "open license" and a "closed license". Licenses 253 contain the rights and conditions that have been granted to a usage device, such as a client, and are digitally signed by the issuer, namely the license servers 220 and 260, in the present example. License 253 is deemed authentic if the signature of the issuing license server can be trusted and verified. License 253 may be an XML or XrML™ file that grants rights and specifies conditions for the use of the protected content.

[0039] Fig. 5 illustrates a license 25e, in accordance with the preferred embodiment. The structure of license 253, whether it be an open license or a closed license as discussed below, consists of unique ID 255a and one or more digital signatures 253c. Grant 253b includes usage-rights, a principal, conditions, state variably an a content specification designating the associated protect content.

[0040] The integrity of license 253 is ensured by the use of digital signature 253c, or another identification mechanism. Digital signature 253c can include the signature code itself, the method of how the signature is computed, the key information needed to verify the signature and also issuer identification information.

[0041] An open license is a license 253 that allows protected content to be used by a client using the software package received from any activation server. In other words, content having an open license associated therewith can be used in any trust zone, in accordance with grant 253b. Thus, referring to Fig. 3, protected content 218 in trust zone 212 may be used by a usage

device such as client 216 in the same trust zone 212 has been issued. In addition, protected content 218 in trust zone 212 may also be used by client 256 in trust zone 252 as long as an open license associated with protected content 218 is issued to client 256. Likewise, protected content 258 in trust zone 252 may be used by client 256 in the same trust zone 252 as long as client 256 has an open or closed license to the content. In addition, protected content 258 in trust zone 252 may also be used by client 216 in trust zone 212 as long as an open license associated with protected content 258 is issued to client 216. Thus, protected content in one trust zone may be used in accordance with the preferred embodiment by a client in a different trust zone (as well as a client of the same trust zone) if an open license is issued to the user, thereby avoiding interoperability problems of having more than one activation process.

[0042] In contrast, a closed license is a license 253 that restricts use of protected content to users which have been activated by an activation server in the same trust zone as the issuing license server and/or other designated trust zones. In other words, protected content associated with a closed license can only be used inside designated trust zones. Thus, in such an instance, referring again to Fig. 3, protected content 218 in trust zone 212 may only be used by client 216 of the same trust zone 212 as long as client 216 is issued a license to do so. In contrast to an open license discussed above, the protected content 218 in trust zone 212 is not consumable by client 256 in trust zone 252 unless trust zone 252 is specifically designated in license 253. Likewise, protected content 258 in trust zone 252 may only be used by client 256 in the same trust zone 252 as long as client 256 is issued a license to do so. As illustrated in Fig. 5, license 253 also includes trust zone indicator 253d. Trust zone indicator 253d can indicate whether license 253 is open or closed. In the case of trust zone indicator 253d indicating a closed license. Trust Zone indicator 253d can indicate one or more predetermined trust zones in which license 253 is valid. Therefore, closed licenses can be

used in one or more trust zones while open licenses can be used in all trust zones.

[0043] As noted above, different business and security models often require multiple activation servers thereby necessitating a multiplicity of activations. However, having numerous activation procedures and resulting software packages creates confusion and problems for the end users and applications utilized by the client to use protected content. For example, if an activated client loses data in an associated software package(s), the client must then go back and reactivate with each of the corresponding activation systems. As can be appreciated, remembering or tracking which activation server(s) were used in activation of a given software package will likely become a significant problem if more than one activation server is present. Thus, DRM system 200 resolves this problem by establishing trust zones, each with an activation server system, and further utilizes two different types of licenses to effectively manage and utilize multiple activation server systems.

[0044] In one implementation of the preferred embodiment, two different types of software packages are provided to clients 216 and 256 by activation servers 210 and 250 during activation. A first type of software package, hereinafter referred to as a "commercial" package, typically allows use of only open licenses. A second type of software package, hereinafter referred to as an "enterprise" package, typically allows use of both open and closed licenses. Commercial software packages and enterprise software packages may merely be considered to be different classes of software packages or separate modules of the same software package that can be selectively activated or enabled in an enterprise application situation so different security policies may exist and one activation system may be used. The commercial software package allows enterprise users the capability to use protected commercial content within the enterprise. The class distinction between a

commercial software package and an enterprise software package may be attained using a unique number identifier such as GUID, an XML tag, a flag or another indication.

[0045] The process of using content in accordance with a license is described in further detail below. In the single activation environment such as DRM system 10 shown in Fig. 1, client environment 60 would "honor" a license if it can determine that the license is valid, and can trust the signature. In accordance with the preferred embodiment, the process of validating and trusting the signature of a license is enhanced with the capability to discern open licenses and closed licenses, based on trust indicator 253d, to allow operation in the manner described above relative to the DRM system 200 of Fig. 3.

[0046] Client device 216 or 256 utilizes the software package obtained during the activation process via activation 210 or 250 server to 1) successfully validate that, through digital signature 253c and trust zone indicator 253d, license 253 is an authentic open license that has been issued in any trust zone or an authentic closed license that has been issued within its own trust zone ; or 2) fail the validation e.g., if the license is not authentic or is a closed license that has been issued outside of its own trust zone.

[0047] The process of granting license 253, whether it be an open or closed license, also includes signing of license 253 with the keys of the software package obtained during the activation process. In the preferred embodiment of the present invention, well known crypto algorithms and public key infrastructure methods may be used to validate digital signatures. Alternatively, any secure mechanism for identification and/or validation can be used. The preferred embodiment leverages the fact that within the same trust zone, the software package for the license server 220 or 260 and the software package for corresponding client 216 or 256 are issued by the same activation server 210 or 250. Therefore, digital signature 253c of license 253

can be verified by recognizing that the certification authority is the same as the one that certified the software package or client 216 or 256. Likewise, if an open license is issued in one trust zone and used in another trust zone, client 216 or 256 recognizes the fact that the certification authority is not the same. Logic in the software package of client 216 or 256 can implement such a decision process, and either accept or reject license 253 depending on which trust zone it was issued from and which trust zones are designated in trust zone indicator 253d. License 253 that is not authentic, i.e. a license which has been tampered with or signed with a signature not issued within the hierarchy of activation servers, is always rejected. License authentication generally is well known. As previously noted, the above operation of an open license and closed license is implemented by the use of digital signature 253c and trust zone indicator 253d as an element of the structure of the license.

[0048] In accordance with the preferred embodiment of the present invention, the process of issuing licenses is enhanced by issuing the open licenses and closed licenses described previously. A policy may be implemented and followed to specify whether the license server would issue an open license for the protected content that allows the content to be used in any trust zone, or issue a closed license for the protected content that is specified to be used within a predetermined trust zone or zones. For example, an administrator of an organization may implement a policy in which use of certain content having a predetermined security level or higher is restricted to only within the organization, while other content having a lower security level may be used outside of the organization. Correspondingly, the administrator may implement a policy in which closed licenses are issued for content having higher security levels while open licenses are issued for content having lower security levels. It should also be understood that in accordance with the preferred embodiment, the protected content is neither open nor closed but is merely encrypted and inaccessible without a proper license.

[0049] Moreover, the method used for determining the type of license issued regarding a particular protected content could be any appropriate means or process using any specified rules or logic. For example, a system may decide that all the protected content within a corporation can only be used internally so that all licenses issued are closed licenses. A system may also decide that the protected content can be used externally and thus, an open license may be issued.

[0050] Fig. 6 illustrates a method of granting licenses in accordance with the preferred embodiment. In step 600, a request for license, to specific content is received by license server 220 or 260. In step 602, the identity and/or location of the source, such as clients 216 or 256, of the request is determined by license server 220 or 260.

[0051] In step 604, the identity of the type and/or location of the requested content is determined. Logic is executed in step 606 to determine the type of license 253 to be generated based on the results of the steps 602 and 604 as well as the identity of the license server receiving the request to thereby effect a license policy For example, rules can be applied to the results. Possibly, all licenses requested by specific users are closed. Licenses to users having a specified security clearance can be open or licenses for certain content can be open. Any set of rules or other logic can be applied in step 606. In step 608, license 253 is generated, either as an open or closed license based on the results of step 606.

[0052] For example, the logic of step 606 can specify that commercial license server would issue open licenses while an enterprise license server would issue closed licenses. Additionally, a commercial license server would typically not issue closed licenses, and an enterprise license server would typically issue open licenses only to authorized users outside of the enterprise's trust zone. An enterprise would typically issue closed licenses for protected content designated for internal use, and open licenses for protected

content designated to be shared outside of the trust zone. Of course, the above logic is an example only, and it should be understood that enterprise any logic can be used to determine whether a license should be open or closed..

[0053] In accordance with another implementation of the preferred embodiment a typical client 216 or 256, such as a client device within an enterprise, is activated twice. In particular, client 216 is activated once by activation server 210 within the enterprise (e.g. an enterprise activation device), and a second time by an activation server 250 as a commercial activation device outside of the enterprise. Client 216 can optionally be activated by other activation servers outside of the enterprise. Activation with other activation servers would allow client 216 to use closed licenses from trust zones other than trust zone 212 as well. By establishing trust zones and utilizing open and closed licenses, together with multiple activations, access and use of protected content can be tailored to various applications and based on various conditions and logic.

[0054] In one implementation of the preferred embodiment, enterprise users will only be activated by the enterprise activation server so that they cannot obtain an enterprise software package from an activation server outside of its trust zone. This again, allows the enterprise system administrator to set the policy, i.e. logic, for activation. For example, the system administrator can then determine who gets activated and how many times they can be activated. The enterprise can also set an expiration date in the software package, and even revoke the software package, i.e., deactivate the user, if desired. However, the same enterprise user could be able to obtain a commercial software package from any commercial activation server to use protected content with open licenses.

[0055] In addition, although any user can obtain a commercial software package from any commercial activation server, the user can be directed to

the particular activation server preferred by the protected content provider. Moreover, a default commerce activation server may be provided which activates clients when no particular activation server is requested so that the activated client is able to use any open license.

[0056] Fig. 4 is a schematic illustration of DRM system 300 in accordance with another embodiment having an optional top-most activation server 310. As shown, top-most activation server 310 is coupled to a plurality of activation servers 320, 330 and 340. Activation servers 320 and 340 define separate trust zones 322 and 342 respectively. Each trust zone 322 and 342 includes a license server and clients of a specific enterprise in the manner previously described. Activation server 330 is in an open commerce zone, e.g. is a commerce server.

[0057] The illustrated embodiment of the present invention provides a hierarchy of trust where top-most activation server 310 serves as an intermediary trusted server that is trusted by activation servers 320, 330, and 340. The provision of top-most activation server 310 allows, for instance, clients in trust zone 322 to use various protected content with an open license in trust zone 342 through activation server 320, without the need for activation server 320 to directly transact with activation server 340 of trust zone 342. For instance, activation servers 320, 330 and 340 may correspond to on-line storefronts, while top-most activation server 310 may be a trusted third entity to which the activation servers 320, 330 and 340 allow access to a particular protected content. Thus, clients in trust zone 322 may use protected content with open licenses in trust zone 342 via activation server 310, although activation server 320 and activation server 340 have not transacted or exchanged information with one another. This hierarchy concept allows protected content with an associated open license in one trust zone to be used by a much larger base of clients since the clients may be in another trust

zone, and the activation servers of the trust zones need not directly transact or provide information to one another regarding a key pair and license.

[0058] It should again be understood that whereas 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 for executing the described function, such as a personal computer, hand held computers, PDAs, 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 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. 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. The varios disclosed components, modules and elements have separate utility and exit as distinct entities.

[0059] While various embodiments in accordance with the present invention have been shown and described, it is understood that the invention, as defined by the appended claims and legal equivalents, 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.

We claim:

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

a first activation device defining a trust zone and being adapted to issue a first software package that enforces usage rights;

a second activation device defining a second trust zone and being adapted to issue a second software package that enforces usage rights;

at least one first license device associated with said first trust zone, said first license device being adapted to generate a license associated with said items and including usage rights specifying a manner of use, said license specifying one or more trust zones in which said license is valid; and

at least one user device associated with said first trust zone, said user device being adapted to receive said first software package, receive said license associated with said items, and to use said items in accordance with said license.

2. The rights management system of claim 1, wherein said items are digital content.

3. The rights management system of claim 2, wherein said license is one of an open license that specifies that said digital content can be used in accordance with the usage rights by user devices having said first software package or said second software package, and a closed license that permits said digital content to be used in accordance with the usage rights only by user devices having said first software package.

4. The rights management system of claim 2, wherein said software package includes a public and private key pair.

5. The rights management system of claim 4, wherein said software package includes a content rendering application.

6. The rights management system of claim 5, wherein said at least one license device is a plurality of license devices that are each associated with one of said first trust zone and said second trust zone, each of said plurality of license devices being adapted to generate a license associated with said items.

7. The rights management system of claim 6, wherein said at least one user device is a plurality of user devices associated with one of said first trust zone and said second trust zone, each of said plurality of user devices being adapted to receive one of said first or second software packages, receive said license associated with said at least one items, and to use said items in accordance with said license.

8. The rights management system of claim 1, wherein said license is an open license that allows said items to be used in by user devices having the first software package or the second software package.

9. The rights management system of claim 1, wherein said license associated with said items is a closed license that allows said items to be used only by user devices having the second software package.

10. The rights management system of claim 9, wherein said license associated with said items is a closed license that allows said items to be used only by user devices having the first software package and by user devices having a software package from specified trust zones.

11. The rights management system of claim 1 further comprising a second license device associated with said second trust zone and wherein

said software package is a commerce software package that allows said at least one device to use said items having an open license that was issued by either of said first license device or said second license device.

12. The rights management system of claim 1, wherein at least one of said first software package and said second software package is an enterprise software package that allows said at least one user device to use said items having a closed license only in said first trust zone.

13. The rights management system of claim 1, wherein at least one of said first software package and said second software package is an enterprise software package that allows said at least one user device to use said items having a closed license only if said license was generated in said first trust zone.

14. The rights management system of claim 3, further comprising a top-most activation device that provides a top level software package to said first and second activation devices.

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

a plurality of activation devices, each activation device defining a trust zone and being adapted to issue a software package that enforces usage rights to control use of said items;

at lease one license device associated with each of said trust zones, each of said of license devices being adapted to generate a license associated with said items and having usage rights specifying a manner of use, said license also including a designation as one of an open and closed license; and

a plurality of usage devices each of usage devices being associated with one of said trust zones and being adapted to receive said software

package, receive said license associated with said items, and to use said items in accordance with said license.

16. The rights management system of claim 15, wherein said license associated with said items is an open license that allows said items to be used in any of said trust zones.

17. The rights management system of claim 15, wherein said license associated with said items is a closed license that allows said items to be used only in a predetermined trust zone.

18. The rights management system of claim 17, wherein said predetermined trust zone comprises a plurality of predetermined trust zones.

19. The rights management system of claim 17, wherein said predetermined trust zone is a trust zone of the license device that generated the license.

20. The rights management system of claim 15, further comprising a top-most activation device that provides a software package for enforcing usage rights to said plurality of activation devices that in turn, issue said software package to said user device.

21. The rights management system of claim 15, wherein said software packages include a public and private key pair.

22. The rights management system of claim 15, wherein said items are digital content.

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

a first activation device defining a first trust zone;

a first license device associated with said first trust zone, said first license device being adapted to generate an open license having usage rights associated with a first item;

a second activation device defining a second trust zone, said second activation device being adapted to issue a software package that enforces usage rights to control use of said first item; and

a user device associated with said second trust zone, said user device being adapted to receive said software package from said second activation device, to receive said open license associated with said first item, and to use said first item in accordance with said open license.

24. The rights management system of claim 23, wherein said software package includes a public and private key pair.

25. The rights management system of claim 23, further comprising a second license device associated with said second trust zone, said second license device being adapted to generate a closed license having usage rights associated with a second item, wherein said closed license permits said second item to be used only by said user device.

26. The rights management system of claim 25, wherein said first activation device is further adapted to issue a software package that allows use of said second item in accordance with said closed license.

27. The rights management system of claim 26, further comprising a top-most activation device coupled to said first and second activation devices to provide a software package to said first and second activation devices.

28. The rights management system of claim 23, wherein said items are digital content.

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

defining a first trust zone and a second trust zone, each trust zone having an activation device associated therewith and adapted to issue a software package that enforces usage rights to control use of said items; and

generating a license associated with said items in said first trust zone, wherein said license includes usage rights specifying a manner of use and a specification of at least one of an open license and a closed license that determines whether said items are usable in at least one of said first trust zone and said second trust zone.

30. The method of claim 29, wherein said software package includes a public and private key pair.

31. The method of claim 29, wherein said license is a closed license that restricts use of said items to said first trust zone.

32. The method of claim 29, wherein said license is an open license that restricts use of said items to either of said first trust zone or said second trust zone.

33. The method of claim 29, wherein said items are digital content.

34. A method for enforcing a license granting usage rights associated with a protected item to control use of the protected item within a trust zone comprising the steps of:

determining whether said license was issued in said trust zone or outside of said trust zone;

determining whether said license is an open license or a closed license;

if said license is a closed license issued outside of said trust zone, prohibiting use of said protected item within said trust zone; and

if said license is an open license issued outside of said trust zone, permitting use of said protected item within said trust zone.

35. A license adapted to be associated with a protected item to control use of the protected item, said license comprising:

usage rights that specify a manner of use for said protected item; and

a license classification indicating whether said license is an open license a permitting use of said protected item outside of said trust zone or a closed license prohibiting use of said protected item outside of said trust zone.

36. A license adapted to be associated with a protected item to control use of the protected item within plural trust zones defined by separate activation devices, said license comprising:

usage rights that specify a manner of use for said protected item; and

a trust zone designation indicating one or more trust zones in which said license is valid.

37. A method of generating a license for a protected item, said license including usage rights specifying a manner of use for said protected item within plural trust zones defined by separate activation devices, said method comprising the steps of;

receiving a request from a user device for a license;

identifying the user device;

identifying the item;

applying logic to the result of said identifying steps to determine if said license should be an open license valid in each of said trust zones or a closed license valid in only predetermined ones of said trust zones; and

generating said license as an open or closed license in accordance with the result of said applying step.

38. The method of claim 37, wherein said applying step comprises generating a closed license if said protected item is determined to be used only internally within an organization.

39. The method of claim 37, wherein said applying step comprises generating an open license if said protected item is determined to be used internally within an organization, and externally outside said organization.

40. The method of claim 37, wherein said applying step comprises generating a closed license if a security level of said identified item exceeds a predetermined level.

41. The method of claim 37, wherein said applying step comprises generating an open license if a security level of said identified item does not exceed a predetermined level.

42. The method of claim 37, wherein said applying step comprises generating a closed license if a security clearance level of said identified user device is below a predetermined level.

43. The method of claim 37, wherein said applying step comprises generating an open license if a security level of said identified user device is above a predetermined level.

44. The method of claim 37, wherein said applying step comprises generating a closed license if said request is received from a predetermined user device.

45. The method of claim 37, wherein said applying step comprises generating an open license if said request is received from a predetermined user device.

Fig. 1

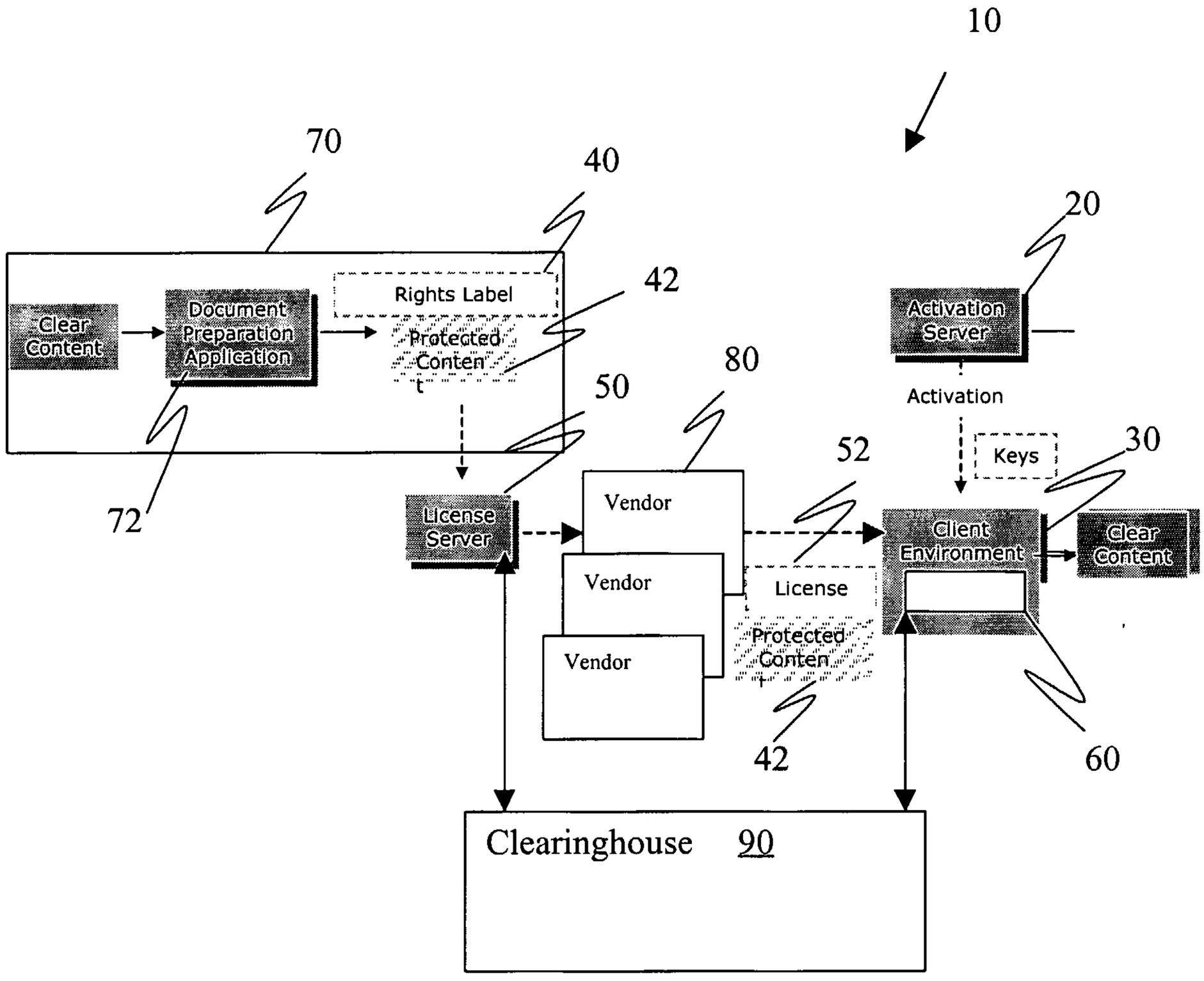

10
70
40
20
Clear Content
Document Preparation Application
Rights Label
Protected Conten t
42
Activation Server
Activation
80
50
52
Keys
30
72
License Server
Vendor
Vendor
Vendor
License
Protected Conten t
Client Environment
Clear Content
42
60
Clearinghouse 90

Fig. 2

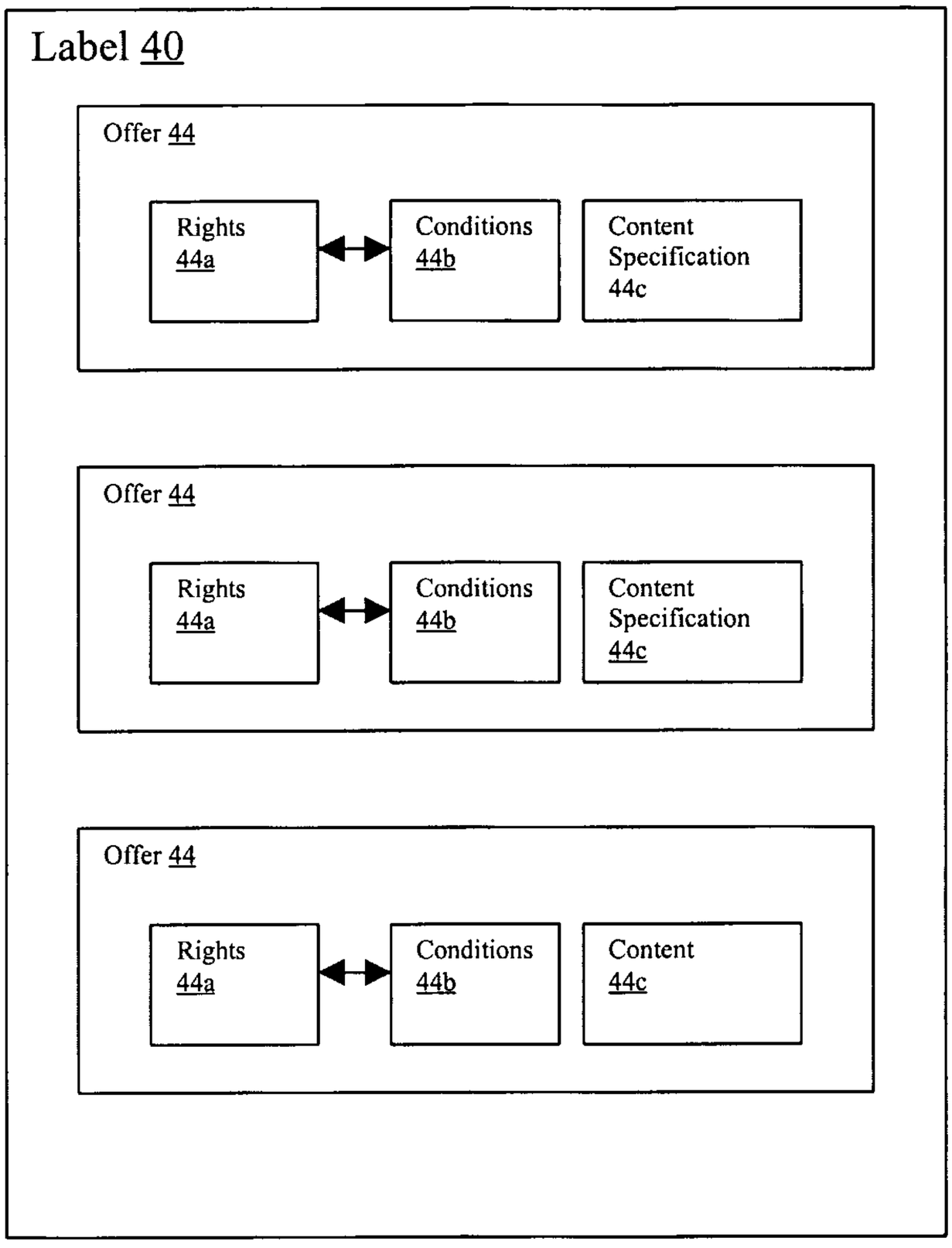

Label 40
Offer 44
Rights 44a
Conditions 44b
Content Specification 44c
Offer 44
Rights 44a
Conditions 44b
Content Specification 44c
Offer 44
Rights 44a
Conditions 44b
Content 44c

Fig. 3

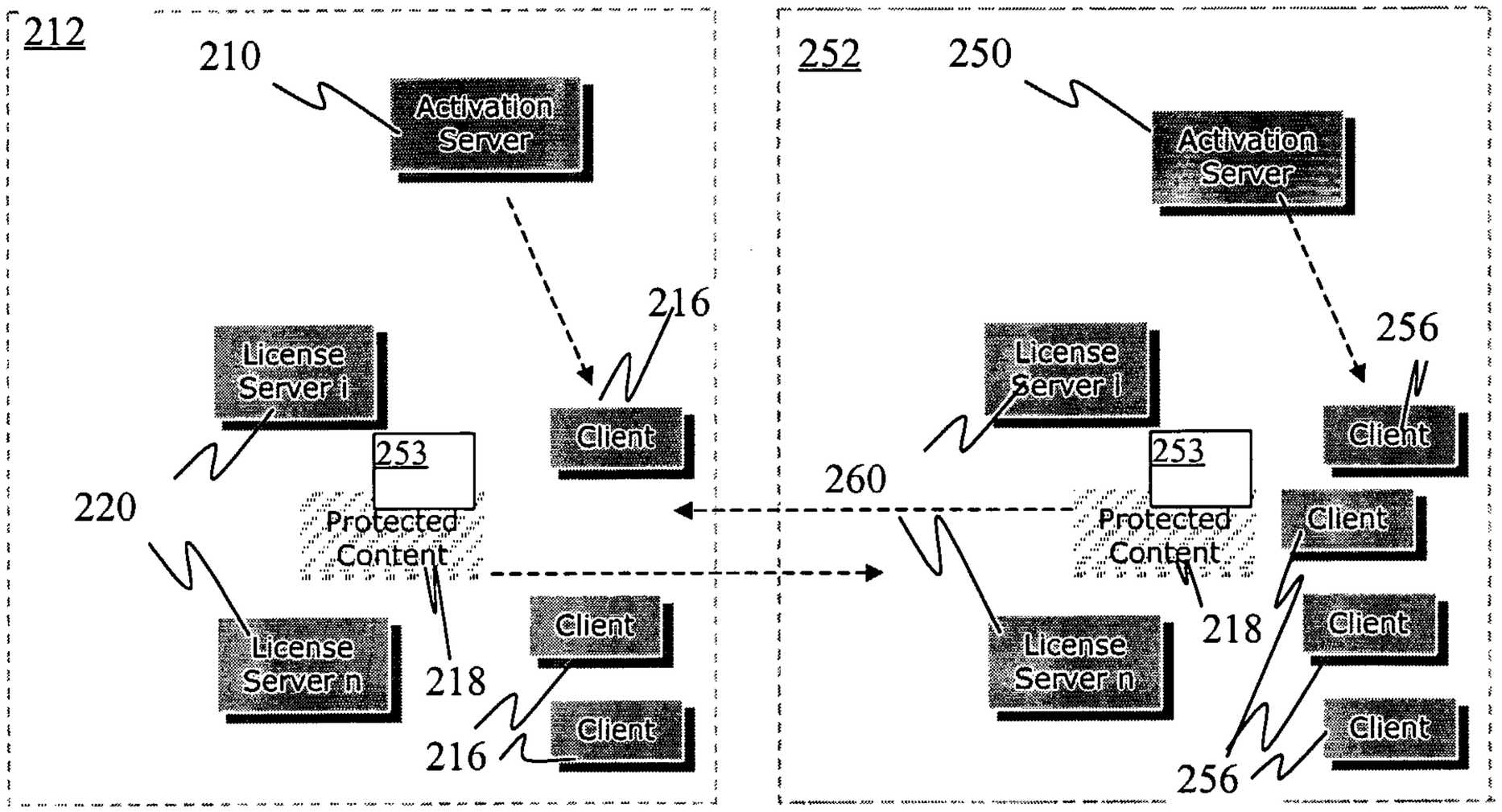

200
212
210
Activation Server
License Server i
220
License Server n
253
Protected Content
218
216
Client
Client
Client
216
252
250
Activation Server
License Server i
260
License Server n
253
Protected Content
218
256
Client
Client
Client
Client
256

Fig. 4

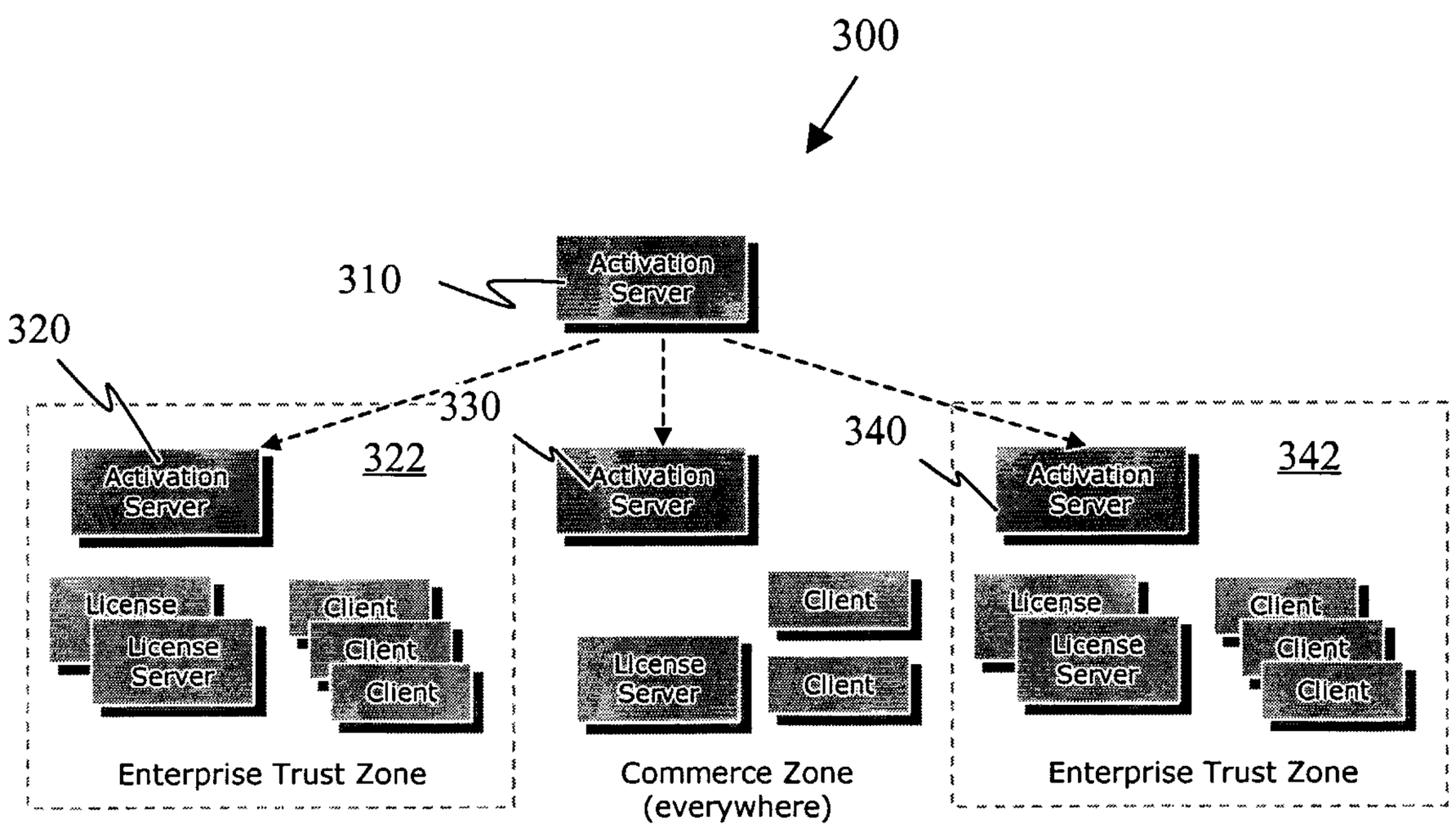

300
310
Activation Server
320
330
340
322
342
Activation Server
Activation Server
Activation Server
License
License Server
Client
Client
Client
License Server
Client
Client
License
License Server
Client
Client
Client
Enterprise Trust Zone
Commerce Zone
(everywhere)
Enterprise Trust Zone

Fig. 5

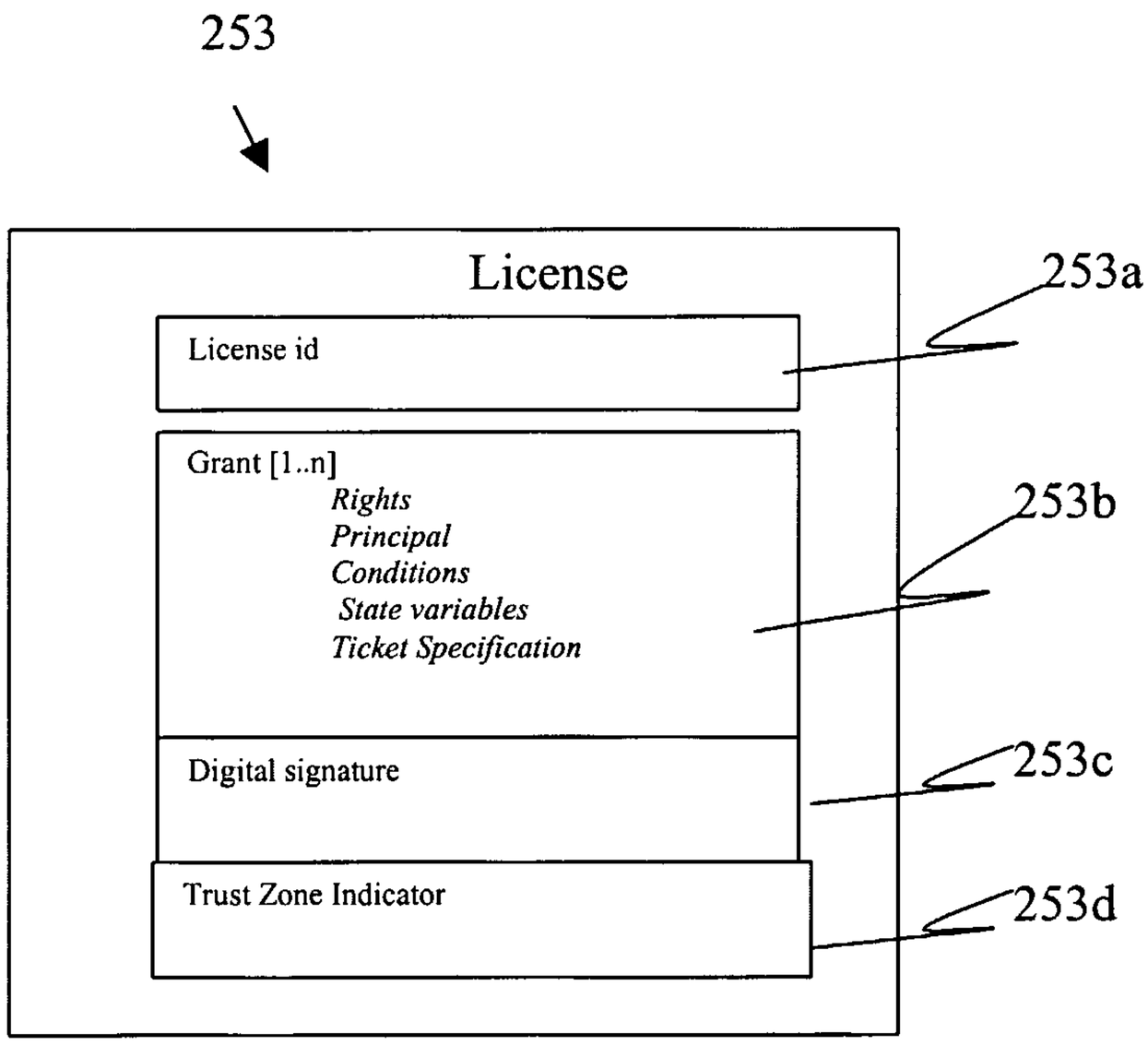
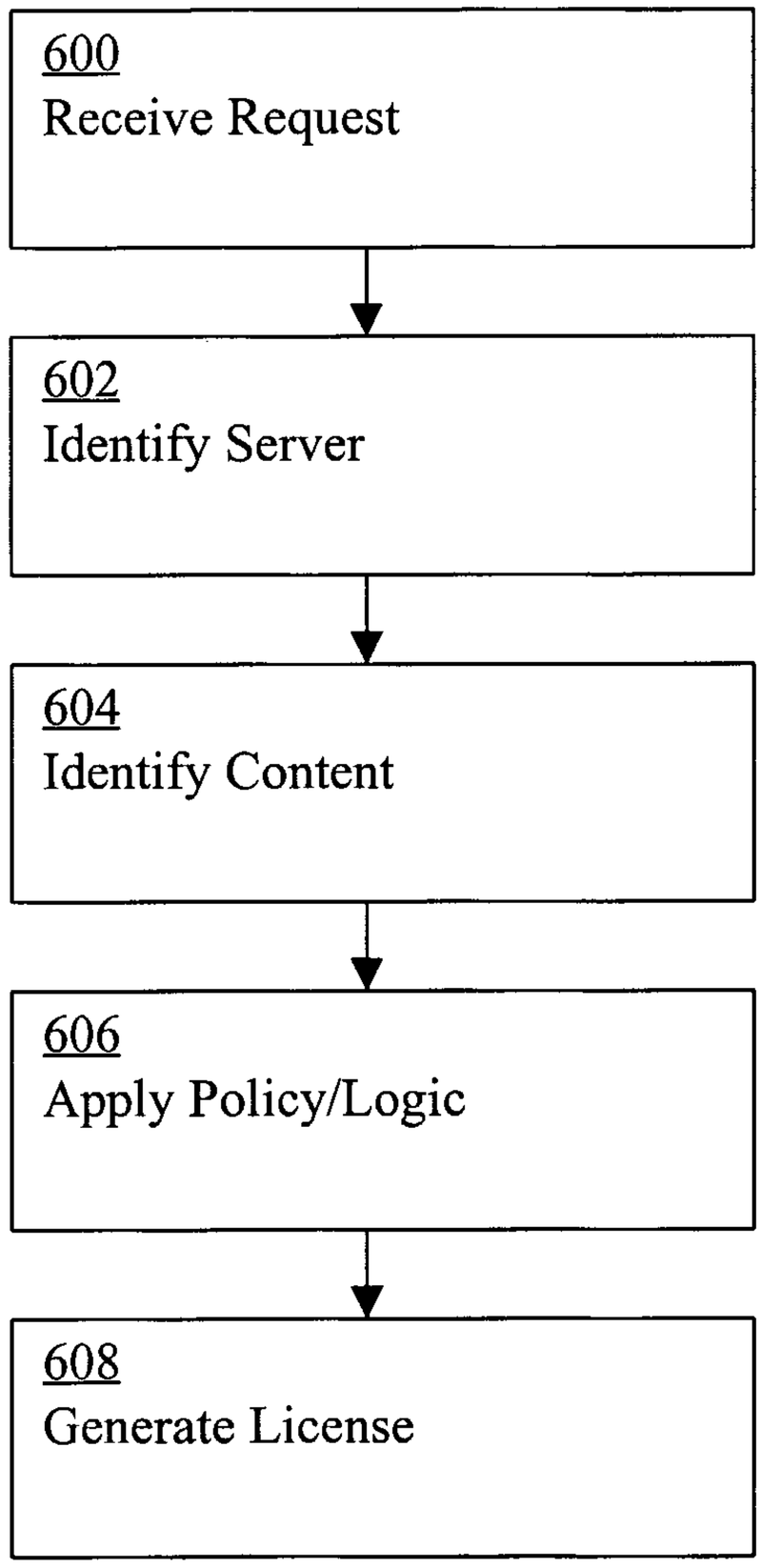
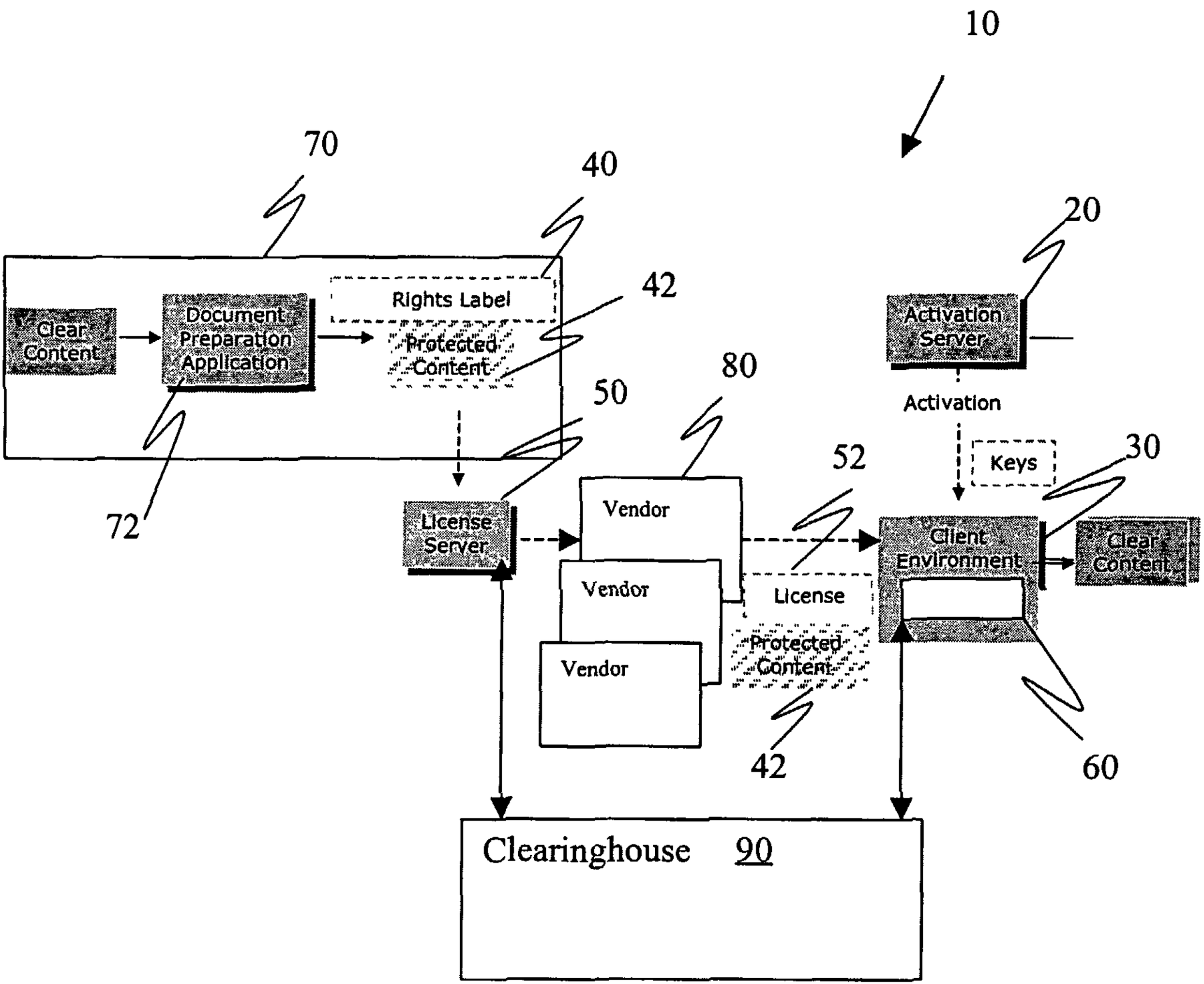

253
License
253a
License id
Grant [1..n]
Rights
Principal
Conditions
State variables
Ticket Specification
253b
Digital signature
253c
Trust Zone Indicator
253d

Fig. 6


600
Receive Request
602
Identify Server
604
Identify Content
606
Apply Policy/Logic
608
Generate License


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