

US PATENT & TRADEMARK OFFICE

PATENT APPLICATION FULL TEXT AND IMAGE DATABASE



(7 of 36)

United States Patent Application**20040024670****Kind Code****A1****Valenzuela, Edgar ; et al.****February 5, 2004**

Rights management system using legality expression language

Abstract

A system and method for managing a legality expression adapted for use in a system for processing said legality expression, including storing on a removable storage medium a legality expression expressed with a legality expression language; reading the legality expression by a device from the removable storage medium; and interpreting the legality expression with an interpreter component. The legality expression language includes respective elements for specifying at least one of an obligation, a prohibition, an intention, and an assertion.

Inventors: **Valenzuela, Edgar;** (*South Gate, CA*) ; **Tadayon, Bijan;** (*Germantown, MD*) ; **Fung, Joseph Zhung Yee;** (*Cerritos, CA*) ; **Wang, Xin;** (*Torrance, CA*)

Correspondence Name and Address: **NIXON PEABODY, LLP**
401 9TH STREET, NW
SUITE 900
WASHINGTON
DC
20004-2128
US

Assignee Name and Address: **ContentGuard Holdings, Inc.**
Wilmington
DE

Serial No.: **425036**
Series Code: **10**
Filed: **April 29, 2003**

U.S. Current Class:**705/35****U.S. Class at Publication:****705/35**

Intern'l Class:

G06F 017/60

Claims

What is claimed is:

1. A method for managing a legality expression adapted for use in a system for processing said legality expression, comprising: storing on a removable storage medium a legality expression expressed with a legality expression language; reading said legality expression by a device from said removable storage medium; and interpreting said legality expression with an interpreter component, wherein said legality expression language includes respective elements for specifying at least one of an obligation, a prohibition, an intention, and an assertion.
2. The method of claim 1, further comprising: specifying one of a legal obligation, a right, a request, a statement, a receipt, a confession, and evidence with said legality expression.
3. The method of claim 1, further comprising: specifying a legal obligation with said legality expression; and enforcing said legal obligation by said device based on said legality expression.
4. The method of claim 3, wherein said obligation is between one or more parties.
5. The method of claim 1, wherein said interpreting step comprises: extracting at least one of syntax information and semantics information from said legality expression.
6. The method of claim 1, further comprising: specifying evidence with said legality expression; and presenting said evidence in a court based on said legality expression.
7. The method of claim 6, further comprising: interpreting said evidence with a reader device in said court, including extracting semantics information from said legality expression to determine a meaning of said evidence; and presenting said meaning of said evidence to at least one of a judge and a jury of said court.
8. The method of claim 1, further comprising: specifying a confession with said legality expression; and presenting said confession as proof based on said legality expression.
9. The method of claim 1, further comprising: specifying a receipt with said legality expression; and presenting said receipt as proof based on said legality expression.
10. The method of claim 3, further comprising: specifying a contract between first and second parties with said legality expression, wherein said legal obligation includes a contractual obligation between said first and second parties.
11. The method of claim 1, further comprising: specifying a right of at least one party with said legality expression.
12. The method of claim 11, wherein said right includes a coupon, and said method comprises: specifying a discount on a purchase of one of digital and non-digital items based on said coupon.
13. The method of claim 12, wherein said non-digital items include physical goods.

14. The method of claim 12, further comprising: downloading said coupon over a communications network onto said removable storage medium; and interpreting said coupon with a reader device in a store.
15. The method of claim 14, wherein said communications network includes at least one of the Internet and an intranet.
16. The method of claim 14, wherein said reader device is included in a checkout register of said store.
17. The method of claim 1, further comprising: specifying an issuer of said legality expression with said legality expression.
18. The method of claim 15, further comprising: digitally signing said legality expression by said issuer; and specifying the digital signature of said issuer with said legality expression.
19. The method of claim 3, wherein said obligation is between first and second parties.
20. The method of claim 19, wherein said first and second parties include individuals.
21. The method of claim 19, wherein one of said first and second parties includes an individual, and the other of said first and second parties includes a party other than an individual.
22. The method of claim 21, wherein said party other than an individual includes one of a country, a state, and a city.
23. The method of claim 21, wherein said party other than an individual includes a company.
24. The method of claim 19, wherein at least one of said first and second parties includes a software component.
25. The method of claim 19, wherein one of said first and second parties includes an individual, the other of said first and second parties includes a court of one of a country, a state, and a city, said legality expression includes a probation rule between said first and second parties, and said legal obligation includes a probation obligation between said first and second parties.
26. The method of claim 19, wherein said legality expression includes a restraining order between said first and second parties, and said legal obligation includes a restraining obligation between said first and second parties.
27. The method of claim 1, further comprising: configuring said removable storage medium as a secure removable storage medium.
28. The method of claim 27, wherein said device comprises a digital signing device, and said method further comprises: employing said removable storage medium in said digital signing device for performing secure digital signing.
29. The method of claim 27, wherein said device comprises a game console, and said method further comprises: employing said removable storage medium in said game console for performing secure lending of a game.

30. The method of claim 27, wherein said device comprises a music player, and said method further comprises: employing said removable storage medium in said music player for performing secure lending of a song.

31. The method of claim 27, wherein said device comprises a music player, and said method further comprises: employing said removable storage medium in said music player for performing secure lending of a song.

32. The method of claim 27, further comprising: employing said removable storage medium in said device for performing secure lending of an item.

33. The method of claim 32, wherein said item includes one of a digital right and digital content.

34. The method of claim 27, wherein said device comprises one of an electronic money device and an electronic check device, and said method further comprises: employing said removable storage medium in said device for performing secure transportation of one of electronic money and an electronic check.

35. The method of claim 1, further comprising: cascading said interpreter component with another interpreter component; and distributing the interpreting of said legality expression between the cascaded interpreter components.

36. The method of claim 1, further comprising: cascading said removable storage medium with another removable storage medium; and distributing said legality expression between the cascaded removable storage medium.

37. The method of claim 35, further comprising: cascading said removable storage medium with another removable storage medium; and distributing said legality expression between the cascaded removable storage medium.

38. The method of claim 1, further comprising: validating said legality expression with a validator component.

39. The method of claim 38, wherein said validating step includes verifying the integrity of said legality expression.

40. The method of claim 38, wherein said verifying step includes determining whether or not said legality expression has been tampered with.

41. The method of claim 38, wherein said interpreting step includes extracting one or more conditions from said legality expression, and said validating step includes determining whether or not one or more of said one or more conditions has been satisfied.

42. The method of claim 38, further comprising: cascading said validator component with another validator component; and distributing the validating of said legality expression between the cascaded validator components.

43. The method of claim 19, further comprising: establishing a trust relationship between said first and second parties based on a list of trusted issuers accessible to said device, said list of trusted issuers including an issuer of said legality expression trusted by said device, whereby said first legality expression can be trusted.

44. The method of claim 19, wherein said legality expression comprises a first legality expression, and said method further comprise: establishing a trust relationship between said first and second parties based on a list of trusted issuers accessible to said device, said list of trusted issuers including an issuer of a second legality expression; and specifying with said second legality expression that an issuer of said first legality expression is authorized to issue said first legality expression, wherein said issuer of said second legality expression is trusted by said device, whereby said first legality expression and said second legality expression can be trusted.

45. The method of claim 1, further comprising: configuring said removable storage medium as a secure removable storage medium by specifying one of authentication and authorization information with said legality expression.

46. The method of claim 45, wherein said authentication information corresponds to an owner of said removable storage medium, and said method further comprises authenticating said holder of said removable storage medium on said device based on said authentication information.

47. The method of claim 46, further comprising: retrieving authentication information corresponding to said holder of said removable storage medium; and comparing said authentication information of said holder with said authentication information of said owner.

48. The method of claim 45, wherein said authentication information includes biometric information.

49. The method of claim 48, wherein said biometric information includes at least one of fingerprint information, toe print information, palm print information, iris pattern information, facial geometry information, voice characteristics information, signature information, and deoxyribonucleic acid (DNA) information.

50. The method of claim 45, wherein said authentication information includes identification information.

51. The method of claim 50, wherein said identification information includes at least one of a username, a password, and a key.

52. The method of claim 45, wherein said authorization information includes rights information.

53. The method of claim 45, wherein said authorization information includes at least one of information regarding who can use said removable storage medium, information regarding how said removable storage medium can be used, and information regarding when said removable storage medium can be used.

54. The method of claim 52, wherein said rights information includes one of a will, a trust, and a power of attorney.

55. The method of claim 48, wherein said device comprises a digital signing device, and said method further comprises: employing said removable storage medium in said digital signing device for performing secure digital signing based on said biometric information.

56. The method of claim 1, further comprising: specifying a behavior of a first object with said legality expression; and transferring said removable storage medium to a second object, whereby said behavior is transferred from said first object to said second object.

57. The method of claim 56, wherein said objects include one of robots, software components, devices, and computers.
58. The method of claim 1, further comprising: downloading said legality expression to one of said removable storage medium and said device over a communications network.
59. The method of claim 58, further comprising: buying said legality expression over said communications network.
60. The method of claim 59, wherein said device comprises a game console and said legality expression comprises a license for a game for said game console.
61. The method of claim 1, further comprising: configuring said removable storage medium to be self-authenticating.
62. The method of claim 1, further comprising: configuring said removable storage medium to be self-authorizing.
63. The method of claim 1, further comprising: distorting a file; specifying with said legality expression a license to play said file in an un-distorted manner and information for un-distorting said file; and playing said file on said device in said un-distorted manner based on said license and said and information for un-distorting said file.
64. The method of claim 63, wherein said file include one of a music file, a movie file, a software file, and a game file.
65. The method of claim 1, wherein said removable storage medium includes one of memory hardware, a memory device, a memory card, a smart card, a dumb card, a credit card, a floppy disk, a hard disk, an optical disk, a compact disk (CD), and a digital versatile disc (DVD).
66. The method of claim 1, further comprising: providing said removable storage medium in one of a cellular phone, a pager, a handheld device, a palmtop device, an Internet appliance, a desktop computer, a laptop computer, a personal digital assistant (PDA), a game console, and a music player.
67. The method of claim 1, wherein said device includes one of a cellular phone, a pager, a handheld device, a palmtop device, an Internet appliance, a desktop computer, a laptop computer, a personal digital assistant (PDA), and a game console, and a music player.
68. The method of claim 1, wherein said legality expression language includes an element for specifying a permission.
69. The method of claim 1, wherein said legality expression language includes a grammar-based legality expression language.
70. A system for managing a legality expression, comprising: means for storing a legality expression expressed with a legality expression language; means for reading said legality expression; and means for interpreting said legality expression, wherein said legality expression language includes respective elements for specifying at least one of an obligation, a prohibition, an intention, and an assertion.
71. The system of claim 70, wherein said legality expression language includes an element for specifying a permission.

72. The system of claim 70, wherein said storing means, said reading means, and said interpreting means comprise devices of a computer system.

73. The system of claim 70, wherein said storing means, said reading means, and said interpreting means comprise computer readable instructions recorded on a medium.

Description

CROSS REFERENCE TO RELATED DOCUMENTS

[0001] The present invention claims benefit of priority under 35 U.S.C. .sctn. 119(e) to commonly assigned, co-pending, U.S. Provisional Patent Application Serial No. 60/375,808 of Wang, entitled "CONTRACTS EXPRESSION LANGUAGE," filed on Apr. 29, 2002, and U.S. Provisional Patent Application Serial No. 60/411,789 of Wang, entitled "CONTRACT EXPRESSION LANGUAGE," filed on Sep. 19, 2002, the entire disclosures of both of which are hereby incorporated by reference herein.

BACKGROUND OF THE INVENTION

[0002] 1. Field of the Invention

[0003] The present invention generally relates to a system for Digital Rights Management, and more particularly a system for management of legality expressions in a Digital Rights Management system.

[0004] 2. Description of Related Art

[0005] One of the most important issues concerning the widespread distribution of digital content, such as documents, music, movies, software, information, and the like, in forms usable by computing devices, via electronic means, and the Internet in particular, is the provision of the ability to enforce the intellectual property rights during the distribution and use of the digital content. Technologies for resolving this problem are referred to as Digital Rights Management (DRM) herein. However, there are a number of issues to be considered in effecting a DRM system, such as authentication, authorization, accounting, payment and financial clearing, rights specification, rights verification, rights enforcement, and document protection issues, to name but a few.

[0006] For example, 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 much easier to copy, modify, and redistribute unprotected digital content with high, quality. Therefore, there is a need for mechanisms to protect digital content.

[0007] Difficulties associated with preventing, or even deterring, people from making unauthorized copies of electronic content 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, are widely recognized. Many attempts to provide hardware-based solutions to prevent unauthorized copying have proven to be unsuccessful. Moreover, the deployment of high bandwidth or broadband communications technologies and the

development of what is presently known as the National Information Infrastructure (NII) is making it more convenient to distribute large documents electronically, including video files, such as full length motion pictures, and this makes it easier to proliferate unauthorized copying and distribution of digital content. Therefore, the need for further development of DRM technologies is becoming a high priority.

[0008] Accordingly, commonly-assigned U.S. Pat. No. 5,634,012 discloses a DRM system for controlling the distribution of digital content, wherein devices of the DRM system can include a repository associated therewith. A predetermined set of usage transaction steps define a protocol used by the repositories for enforcing usage rights associated with the content. Usage rights persist with the content and the usage rights associated with the content comprise a digital work. The usage rights can permit various manners of use of the content, such as a right to view or print or display the content, a right to use the content only once, a right to distribute or redistribute the content, and the like. Such usage rights can be made contingent on payment or other conditions. However, there is a need for systems and methods that enable one or more parties to easily and securely manage, exchange, interpret, enforce, and the like, legality information and that provides flexibility, extensibility, interoperability, ease of use, and online and offline capabilities.

SUMMARY OF THE INVENTION

[0009] The above and other needs are addressed by embodiments of the present invention, which provide an improved system and method for management of legality expressions.

[0010] Accordingly, in one aspect of an embodiment of the present invention, there is provided a system and method for managing a legality expression adapted for use in a system for processing said legality expression, including storing on a removable storage medium a legality expression expressed with a legality expression language; reading the legality expression by a device from the removable storage medium; and interpreting the legality expression with an interpreter component. The legality expression language includes respective elements for specifying at least one of an obligation, a prohibition, an intention, and an assertion.

[0011] Still other aspects, features, and advantages of the present invention are readily apparent from the following detailed description, simply by illustrating a number of exemplary embodiments and implementations, including the best mode contemplated for carrying out the present invention. The present invention is also capable of other and different embodiments, and its several details can be modified in various respects, all without departing from the spirit and scope of the present invention. Accordingly, the drawings and descriptions are to be regarded as illustrative in nature, and not as restrictive.

BRIEF DESCRIPTION OF THE DRAWINGS

[0012] The present invention is illustrated by way of example, and not by way of limitation, in the figures of the accompanying drawings and in which like reference numerals refer to similar elements and in which:

[0013] FIG. 1 illustrates an exemplary Digital Rights Management system on which various embodiments of the present invention can be implemented;

[0014] FIG. 2 illustrates an exemplary Legality Expression Management system that can be implemented with one or more of the devices and subsystems of the system of FIG. 1;

[0015] FIG. 3 is a flowchart for illustrating an exemplary process of trust chaining that can be employed

in the systems of FIGS. 1 and 2-10;

[0016] FIG. 4 illustrates an exemplary embodiment of the Legality Expression Management system of FIG. 2, including a reader/writer device having expression interpretation and validation components and a removable storage device;

[0017] FIG. 5 illustrates an exemplary embodiment of the Legality Expression Management system of FIG. 2, including a card reader device having expression authorization and authentication components that communicate with an interpreter;

[0018] FIG. 6 illustrates an exemplary embodiment of the Legality Expression Management system of FIG. 2, including a card writer device having an expression generation component and expression authorization and authentication components that communicate with an expression interpretation component;

[0019] FIG. 7 illustrates an exemplary embodiment of the Legality Expression Management system of FIG. 2, including a card reader device having expression authorization and authentication components each having an expression interpretation component;

[0020] FIG. 8 illustrates an exemplary embodiment of the Legality Expression Management system of FIG. 2, including a game console having an expressions storage component and a card reader/writer device having expression authorization and authentication components that communicate with an expression interpretation component;

[0021] FIG. 9 illustrates an exemplary embodiment of the Legality Expression Management system of FIG. 2, including a smart removable storage device and a reader/writer device having expression interpretation and validation components;

[0022] FIG. 10 illustrates an exemplary embodiment for cascading of a removable storage medium and that can be employed in the systems of FIGS. 1 and 2-9;

[0023] FIG. 11 is a flowchart for illustrating an exemplary process for expression interpretation and validation that can be employed in the systems of FIGS. 1 and 2-10; and

[0024] FIG. 12 is a flowchart for illustrating an exemplary process for expression authorization and authentication that can be employed in the systems of FIGS. 1 and 2-10.

DETAILED DESCRIPTION OF THE INVENTION

[0025] A system and method for management of legality expressions are described. In the following description, for purposes of explanation, numerous specific details are set forth in order to provide a thorough understanding of the present invention. It is apparent to one skilled in the art, however, that the present invention can be practiced without these specific details or with equivalent arrangements. In some instances, well-known structures and devices are shown in block diagram form in order to avoid unnecessarily obscuring the present invention.

[0026] As noted above, authentication, authorization, accounting, payment and financial clearing, rights specification, rights verification, rights enforcement, and document protection issues should be addressed by a Digital Rights Management system. Commonly-assigned U.S. Pat. No. 5,530,235, No. 5,629,980, No. 5,634,012, No. 5,638,443, No. 5,715,403, No. 6,233,684, and No. 6,236,971, the entire disclosures of all of which are hereby incorporated by reference herein, disclose DRM systems

addressing these and other issues.

[0027] The present invention includes recognition that various types of cards can be used to store various types of information. For example, access control cards can store information about an identity of a person, which can be read by a card reader to authenticate the person. After authentication, an authorization phase can be employed to determine whether or not the authenticated identity has been granted a right to act, for example, on a resource. Authorization can be determined by accessing a data store or knowledge base, which can be maintained within a secure system that can be used to enforce one or more permissions or rights associated with the resource. The results of the authorization can be used determine a level and/or manner of access to the resource.

[0028] Such permissions or rights can be hard-coded on a suitable card. The present invention includes recognition, however, that hard-coding permissions or rights on a card can raise problems relating to security risks, revocation of rights, and the like. For example, as described in U.S. Pat. No. 4,816,658, a card reader can employ a central controller to determine authorization. When the central controller is down or unreachable or the domain of the central controller is outside of access control, the card reader can assume that the person is authorized or unauthorized by default, possibly logging the decision and sending the data to the central controller once contact is re-established. Similarly, U.S. Pat. No. 4,868,376 is directed to an intelligent portable interactive personal data system and U.S. Pat. No. 6,275,991 is directed to an infrared (IR) transmitter with integral magnetic-stripe credit card reader. However, such systems can fail to grant access when access should be granted or can grant access when access should not be granted.

[0029] In addition, systems based on card reader technologies also can have a difficult time with interoperability. For example, sharing of authorization information between various business entities can entail synchronizing systems and/or communications and a need for a shared understanding of the formats used for communicating the authorization information between such systems.

[0030] For example, customers of a Video Rental Store can receive a generic membership card that can be used to identify the cardholder. The Video Rental Store can provide various membership types or subscriptions, for example, a Super Movie Watcher club, a Movie a Week Club, and the like. The Video Rental Store can employ a database to specify one or more membership types for each customer. Then, when a customer rents a movie, a suitable card reader can scan the card of the customer to identify the cardholder. Once identified, the customer can be afforded various pricing levels based on the membership type of the customer.

[0031] Now assume that a Pizza Parlor desires to give a \$2 discount to members of the Super Movie Watcher club of the Video Rental Store. The Pizza Parlor, however, typically would have to contact the Video Rental Store to determine whether a customer with a card from the Video Rental Store is a member of the Super Movie Watcher club. Thus, the Video Rental Store typically would need to provide some sort of service to allow the Pizza Parlor to obtain such information.

[0032] Accordingly, the Pizza Parlor would have to depend on the availability of such a membership lookup service of the Video Rental Store to provide the \$2 discount to members of the Super Movie Watcher club. However, if the membership lookup service is down or inaccessible, the Pizza Parlor would not be able to determine whether a customer is entitled to the \$2 discount.

[0033] The Pizza Parlor also may have to become familiar with and employ any Application Programming Interfaces (APIs) used by the Video Rental Store for providing the membership lookup service. In addition, other businesses having similar business relationships with the Pizza Parlor may require the Pizza Parlor to employ various other types of APIs. The \$2 discount program could quickly

become an unprofitable and time-consuming proposition.

[0034] The Video Rental Store can embed information about the membership types of a cardholder on the membership card, such that the Pizza Parlor can scan the card to determine whether the cardholder is in the Super Movie Watcher club. The Pizza Parlor, however, would have to understand the organization and/or meaning of the data format used by the Video Rental Store for embedding the membership information. For example, the Video Rental Store might employ a data format based on strings to specify the different membership types, positionally associate bits with membership types, and the like, and which would have to be communicated to the Pizza Parlor.

[0035] In addition, the Pizza Parlor may have one or more business relationships with other local businesses. Accordingly, if the Pizza Parlor desires to provide discounts to customers of such businesses, the Pizza Parlor typically would have to become familiar with and handle the numerous types of other possible data schemes.

[0036] The present invention, thus, includes recognition of the above and other problems associated with sharing of authorization and authentication information and that the need for extensibility of authorization and authentication schemes using card and card reader technologies can entail a relatively large business investment and time-consuming processes. For example, an authorization or authentication component typically would have to be updated when one or more rights are issued.

[0037] In the case of an access control security system, when someone is granted rights to access a new area of the security system, typically a change would have to be programmed into the authorization component or the authorization component would have to be configured to directly trust the entity that placed the authorization information on a card. Advantageously, problems associated with trusting third parties are addressed by the exemplary embodiments. Similarly, addressing the extensibility issues typically would include major changes for each business and business partners of each business.

[0038] In addition, the exemplary embodiments address problems related to coupons and coupon distribution. For example, coupons can be distributed using both hard copy sources, such as newspapers, magazines, booklets, and the like, and electronic sources, such as the Internet, over e-mail, and the like. However, consumers typically have to print such coupons to be used when the consumers go to a store, such as a grocery store, and the like.

[0039] The consumers also can receive coupons when at a checkout stand, for example, printed on a receipt. However, the consumers typically end up losing such coupons, forgetting to use such coupons, and the like. Advantageously, the exemplary embodiments provide an interoperable system that can enable the consumers to get digital or electronic coupons from one entity, such as an Internet site, and the like, and take the coupons to a physical redemption location, such as a store, and like, and vice versa.

[0040] Thus, the exemplary embodiments, advantageously, empower removable storage media, smart cards, card readers, card writers, and the like, with a legality expression (LE) and Rights Expression (RE) processing capability to address the above and other problems.

[0041] Referring now to the drawings, wherein like reference numerals designate identical or corresponding parts throughout the several views, and more particularly to FIG. 1 thereof, there is illustrated a Digital Rights Management system 100 that can be used in connection with the described exemplary embodiments to specify and enforce usage rights for content, services, or other property. In FIG. 1, the Digital Rights Management system 100 includes a user activation component in the form of an activation server 110 that issues a set of public and private key pairs 112 to a content user in a

protected fashion. Typically, when the user uses the Digital Rights Management system 100 for the first time, the user installs software that, for example, works with, or includes, a rendering application for a particular content format.

[0042] The software is installed in a client environment 120, for example, such as a computing device associated with the user. The software can be part of the Digital Rights Management system 100 and can be used to access protected content 134. After the installation, the software can be activated. During the activation process, some information is exchanged between the activation server 110 and the client environment 120. A client software component 122 can be downloaded and installed in the client environment 120. The client software component 122 can be tamper resistant and can include the set of public and private key pairs 112 issued by the activation server 110, as well as other components.

[0043] A rights offer 132 can be associated with the protected content 134 and can specify usage rights 132A that are available to an end-user, for example, when one or more corresponding conditions 132B are satisfied. A license server 140 manages the encryption keys 112 and issues a license 142 for the protected content 134. The license 142 can embody the actual granting of the usage rights 132A to the end user. For example, the rights offer 132 may grant the end user the right to view the protected content 134 on the condition of payment of a fee of five dollars, and the right to print the protected content on the condition of payment of a fee of ten dollars. The license 142 can be issued for the view right when the five dollar fee has been paid and/or for the print right when 10 dollar fee has been paid. The client component 122 interprets and enforces the rights that have been specified in the license 142.

[0044] Clear content 136, such as unprotected content, and the like, can be prepared, for example, with an application 138, such as a document preparation application, installed on a computer 130 associated with a content publisher, a content distributor, a content service provider, or any other suitable party. Preparation of the clear content 136 can include specifying the usage rights 132A and the conditions 132B under which the clear content 136 can be used, associating the rights offer 132 with the clear content 136, and protecting the clear content 136 with, for example, a cryptography algorithm to generate the protected content 134. A rights language, such as XrML, eXtensible Access Control Markup Language (XACML), Open Digital Rights Language (ODRL), and the like, can be used to specify the rights offer 132. However, the rights offer 132 can be specified in any suitable manner. The specifying of rights information can include to creating, deriving, or other wise utilizing information that relates to rights expressions. Also, the rights offer 132 can be in the form of a pre-defined specification, profile, template, and the like, that can be associated with the protected content 134. Accordingly, the process of specifying the rights offer 132 can include any suitable process for associating rights, conditions, and the like, with content. The rights offer 132 associated with the protected content 134 and the encryption key 112 used to encrypt the clear content 136 can be transmitted to the license server 140.

[0045] A typical workflow for the Digital Rights Management system 100 can include a user operating within the client environment 120 being activated for receiving the protected content 134 by the activation server 110. The activation process results in the public and private key pair 112, and, for example, some user and/or machine-specific information, and the like, being downloaded to the client environment 120 in the form of the client software component 122. The activation process can be accomplished, for example, at any suitable time prior to the issuing of the license 142.

[0046] When the user wishes to use the protected content 134, the user makes a request for the protected content 134. For example, the user might browse a Web site running on a Web server 150, using a browser installed in the client environment 120, and attempt to download the protected content 134. During this process, the user may go through a series of steps possibly including a fee transaction, such as in the sale of content, other transactions, such as collection of information, and the like. When the

appropriate conditions and other prerequisites, such as the collection of a fee and verification that the user has been activated, are satisfied, the Web server 150 contacts the license server 140, for example, through a secure communications channel, such as a channel using a Secure Sockets Layer (SSL). The license server 140 then generates the license 142 for the protected content 134 and the Web server 150 downloads both the protected content 134 and the license 142. The license 142 can include the appropriate usage rights of the usage rights 132A and can be downloaded from the license server 140 or an associated device. The protected content 134 can be downloaded from the computer 130 associated with a publisher, distributor, or other party. The rights offer 132 can be persistent and remain associated with the protected content 134.

[0047] The client software component 122 in the client environment 120 can then proceed to interpret the license 142 and allow use of the protected content 134 based on the rights 132A and the conditions 132B specified in the license 142. The interpretation and enforcement of the usage rights, for example, are further described in commonly-assigned U.S. Pat. No. 5,530,235, No. 5,629,980, No. 5,634,012, No. 5,638,443, No. 5,715,403, No. 6,233,684, and No. 6,236,971. The above steps can take place sequentially, approximately simultaneously, in various orders, and the like.

[0048] The Digital Rights Management system 100 addresses security aspects of protecting the protected content 134. In particular, the Digital Rights Management system 100 can authenticate the license 142 that has been issued by the license server 140. One way to accomplish such authentication is for the client software component 122 to determine if the licenses 142 can be trusted. In other words, the client software component 122 can include the capability to verify and/or validate the cryptographic signature, or other identifying characteristic of the license 142. During the activation step described above, the client environment 120 and the license server 140 can receive the set of keys 112, for example, in a tamper-resistant software package that can include other components, such as the client software component 122 for the activated client environment 120 to verify the signature of the license 142.

[0049] The Digital Rights Management system 100 is of an exemplary nature and can be implemented in numerous other equivalent arrangements. For example, the license 142 and the protected content 134 can be distributed from different entities. As another example, the rights offer 132 can be associated with the protected content 134 by a party other than the party preparing the protected content 134. As a further example, a clearinghouse 160 can be used to process payment transactions and verify payment prior to issuing the license 142. Moreover, the various processes and transactions can be performed, for example, via online and/or offline environments and/or combinations thereof. For example, an end user could download content to a computer and then transfer the content from the computer to a personal digital assistant (PDA). The end user could then buy a license for the content, for example, via a supermarket kiosk, a cash register, a prep-paid license card, and the like, and then transfer the license to the PDA. The end user could then activate the content for use on the PDA and/or the computer. In such an offline scenario, the various devices can, but need not, communicate directly with one another and information can be exchanged in any suitable manner, such as by physically moving media between the devices.

[0050] The exemplary embodiments employ legality expressions, for example, based on a Legality Expression Language (LEL) and a Rights Expression Language (REL), such as eXtensible Rights Markup Language (XrML)-based language, and the like. The Legality Expression Language, for example, can include a broad class of expression languages related to any suitable legal instrument, item, or object, such as contract, promise, right, request, will, binding language, exchange, condition, term, servitude, easement, covenant, and the like. The terms and expressions can be set by any suitable entity, and need not be based on a specific law, rule, and the like.

[0051] A useful legality expression can include a syntactically and semantically correct construct based on a defined grammar, such as a Legality Expression Language. Advantageously, the Legality Expression Language can be employed to convey information or data related to direct or indirect, implied or explicit legal issues, laws, and the like. For example, the Legality Expression Language can be employed to express rights, obligations, official statements, requests, declarations, oaths, logs, and the like. The Legality Expression Language, for example, can be employed to express conditions concerning content, services, behavior, and the like. The Legality Expression Language, for example, can be employed to express past, present or future actions or thoughts or beliefs, and the like. The Legality Expression Language, for example, can be employed to express wills, ownerships, servitudes, promises, offers or counter-offers, contracts, negotiations, prohibition, exclusivity, Intellectual Property (IP) ownership, stock ownership, and the like.

[0052] Accordingly, the Legality Expression Language can include elements for specifying an obligation, for example, that a principal must perform an act, a prohibition, for example, that a principal must not perform an act, an intention, for example, that a principal wants to perform an act, an assertion, for example, that a principal does perform an act, and a permission, for example, that a principal may perform an act. In the exemplary embodiments, an act can include the process or state of doing or performing something, an assertion can include a declaration of performing some act, an intention can include a course of action that one intends to follow, an obligation can include a commitment that requires someone to perform some act, a permission can include a right, a principal can include an encapsulation of the identification of an entity involved in the performing of an act, and a prohibition can include a requirement that forbids someone to perform an act.

[0053] The set of Legality Expression Languages of the exemplary embodiments, for example, can include Rights Expression Languages (RELs), Contract Expression Languages (CELs), Request Expression Languages (RqELs), and the like. Exemplary legality expressions, for example, written in XrML, are provided as an Appendix. A Data Dictionary can be employed with an Expression Language, such the Legality Expression Language. An Expression Language can be based on a grammar that defines relationships, rules, and the like, within parts or components of the Expression Language.

[0054] Advantageously, the Legality Expression Language can be employed in a variety of applications according to the exemplary embodiments. For example, the Legality Expression Language can be employed for specifying authentication data, such as credentials, and the like, biometric information that expresses prints, such as fingerprints, toe prints, palm prints, iris patterns, facial geometry, behavior, voice characteristics, signatures, deoxyribonucleic acid (DNA), and the like. Such authentication data also can include identifiers, such as usernames and passwords, keys, identifications (IDs), associations, and the like.

[0055] Advantageously, the Legality Expression Language can be employed for specifying authorization data including rights, such as wills, trusts, powers of attorney, and any suitable other type of rights, and the like, that have been granted to or denied from a given party, person, groups of persons, entity, entities, and the like.

[0056] Advantageously, contracts that can include any suitable instrument used in a legal arena, and the like, also can be expressed with the Legality Expression Language, such as the Contract Expression Language, and the like.

[0057] Advantageously, the Legality Expression Language can be employed for specifying Official statements, for example, including confessions, such as a confession by an arrested person, claims of responsibility, such as party claiming to take responsibility for bills owed by another party, testimonies, such as a testimony from a witnesses in a trial, testimonials, such statements from individuals claiming

that a product helped the individuals lose weight, advice, such as government officials advising the President not to go to war, acknowledgements, such acknowledgement that a package was received, opened, or used, an acknowledgement from a notary public, an acknowledgement of completion, affidavits, notarizations, oaths, and the like.

[0058] Advantageously, the Legality Expression Language can be employed for specifying requests, results, logs, and the like, from any suitable party to any other suitable party, such as requests made by one server to another, or from any suitable hardware or software, from a person to the police, from one country to another, and the like. Similarly, the results can be of any suitable type, for example, such as results of tests, research, elections, and the like. The logs also can be of any suitable type, for example, such as computer logs, building access logs, and the like.

[0059] The legality expressions can be relatively simple or complex, for example, depending on factors, such as the richness, the built-in coverage, the flexibility, the extensibility, and the like, of the corresponding Expression Language. Similarly, the legality expressions can be relatively simple or complex, for example, depending on the complexity of the model for which the legality expressions are used.

[0060] In an exemplary embodiment, the legality expressions can be expressed in various forms. For example, the legality expressions can be expressed as binary-encoded sequences that target resource-constrained applications or devices. Multi-level Legality Expression Language constructs can be employed to describe complex legal information, such as for managed distribution of digital or physical items or resources, and the like, or to describe complex business models, and the like. The legality expressions can be encoded in any suitable manner, for example, using symbols, objects, colors, and the like. The legality expressions, for example, can employ sounds, other representations, and the like, that can be undetectable by human senses, but that can be detected by suitable machines, and the like.

[0061] In an exemplary embodiment, a Expression Language interpreter can be employed, for example, including any suitable component that can extract semantics from a legality expression. For example, a legality expression language interpreter can be based on a Rights Expression Language (REL) interpreter, such as an XrML interpreter, and the like, and can be employed to determine authorization, authentication, and the like. Such an interpreter, for example, can be requested to determine whether or not a particular principal has the right to act on a particular resource.

[0062] Such an interpreter, for example, can further determine whether or not a legality expression or set of legality expressions give a specified principal a right to act on a specified resource. For example, an XrML interpreter can be presented with the following exemplary license and then queried to determine whether or not Jon Doe can print the e-book "XrML Unleashed." The interpreter then would analyze the exemplary license to determine that John Doe can print the book "XrML Unleashed," for example, by providing a Yes or affirmative result.

```
1 <license> <grant> <keyHolder licensePartId="John Doe"> <info> <dsig:KeyValue>
<dsig:RSAKeyValue>
<dsig:Modulus>Fa7wo6NYfmvGqy4ACSWcNmuQfbejSZx7aCibIgkYswUeTCrmS
Oh27GJrAI5SS7TYZzSfaSOxR9IZdUEF0ThO4w==</dsig:Modulus>
<dsig:Exponent>AQABAA==</dsig:Exponent> </dsig:RSAKeyValue> </dsig:KeyValue> </info>
</keyHolder> <ex:print/> <ex:digitalWork> <ex:locator> <nonSecureIndirect
URI="http://www.CompnayA.com/XrMLUnleashed.spd"/>- ; </ex;locator> </ex:digitalWork> </grant>
</license>
```

[0063] The interpretation process can increase in complexity as the legality expressions become richer,

for example, in the case of dependant legality expressions. For example, a legality expression can have a prerequisite condition that stipulates that the principal can have some one or more other rights or legal obligations. The legality expressions that satisfy any suitable prerequisite condition also can have prerequisite conditions, such that the interpretation can entail interpreting many legality expressions to determine authorization, authentication, and the like. The interpretation process also can include extracting syntax and semantics information from the legality expressions.

[0064] The Legality Expression Language interpreter, for example, also can include a Contracts Expression Language (CEL) interpreter, and the like. A Contracts Expression Language interpreter, for example, can use contract expressions, extract the semantics information from the contract expressions, form a combined set of rules that can be followed, and the like. Advantageously, the Contracts Expression Language interpreter, for example, can be used in an automated system, wherein the contracts expressions, for example, can serve as instructions as to how the automated system can behave.

[0065] The process of interpretation can yield conditions that can be met immediately, prior, during, or after some action, for example, such as the exercise of a right or legal obligation at some specific time, at a triggering point, and the like. For example, legality expressions can include conditions on the exercise of a right or legal obligation. Examples of conditions on rights or legal obligations can include validity intervals, exercise limits, fees, generic approval seeking, tracking, transfer restrictions on locations, render restrictions, territories of use, and the like.

[0066] For example, a legality expression can be used to specify that a user can view the book "XrML Unleashed" on a condition or legal obligation that the user pays \$3. Thus, the fee of \$3 can be a condition or legal obligation that can be specified to be met before the user can view the book. A condition or legal obligation validation component can be employed, for example, to verify that the user has paid the fee. The validation component, for example, also can provide an interface or mechanism for the user to pay the fee, can check to determine whether the user pays the fee or has paid the fee, and the like. Advantageously, the validation components, for example, also can be employed to enforce or verify contractual agreements or any suitable other legality constraints, and the like.

[0067] Advantageously, the exemplary embodiments provide a mechanism for transporting, securing, managing, and the like, Legality Expression Language-based expressions. The exemplary embodiments can be used to create a link between devices that are disconnected, such as devices used in the online world, such as Internet servers, and the like, and devices used in the physical world, such as cash registers, client devices, home appliances, automatic teller machines, court evidence systems, cars, game consoles, music players, and the like.

[0068] The exemplary embodiments enable end users to use content, services, and features on multiple devices using a secured legality expression, such as a license or contract. In an exemplary embodiment, a removable storage medium, such as a card or key, and the like, can be configured to store a legality expression. When a user wishes to use given rights specified by the legality expression on another device or present some obligation to another device, the user can employ the removable storage medium on such a device.

[0069] The use of a removable storage medium with legality expressions provides numerous advantages. For example, the exemplary embodiments can be used to support a trusted offline transfer of legality expressions, such as rights, licenses, and contracts between entities, and the like. Advantageously, a secure offline solution for lending between devices can be provided. For example, a user can lend to a friend or to other devices in a home or office of the user, and the like.

[0070] In an exemplary embodiment, a legality expression can be employed for specifying the lending of any suitable item or thing, for example, including digital and non-digital items or things. For example, an exemplary system can be configured for loaning of a right to use public transportation specified via a legality expression. Such an exemplary system can be configured to be a secure or trusted system and can employ secure removable storage devices that can be read or written by a secure or trusted reader/writer device. Advantageously, such a right can be sold to a person and, for example, can specify use of a metropolitan transportation system (metro) for one month. The right can be stored on the removable storage device, such a metro card, and the like. Then, when a cardholder goes to the metro, the card reader with an interpreter can check to see if the cardholder has the right to get on the metro.

[0071] Advantageously, a person having such a right to use the metro can transfer the right to a friend so that the friend can ride the metro. In an exemplary embodiment, such a transfer can be made between secure or trusted cards, such as smart card devices, and the like, by taking the cards to some trusted point of transfer, such as a secure or trusted reader/writer device that takes the rights from one card and places them on the other card.

[0072] The exemplary embodiments support secure transport of legality expressions from one device to another, advantageously, enabling models in which one device can use a particular legality expression at a time, but multiple devices can use the same legality expression at different times. For example, with the exemplary embodiments, a user can watch a movie on a laptop computer during a long trip, and also watch the same movie on a home DVD player when at home.

[0073] Advantageously, the exemplary embodiments provide an interoperable and secure method of sharing legality information. For example, in an exemplary embodiment, a removable storage medium can be configured to include legality expressions expressed in a standardized Legality Expression Language to enable different businesses to interoperate relatively easily, because the different businesses can share the Legality Expression Language. Advantageously, the need to employ many different proprietary data formats can be eliminated.

[0074] The exemplary embodiments, advantageously, support multi-tier trust. Multi-tier trust can include a method of making trust decisions based on trust chaining, for example, wherein a friend of a friend is a friend. For example, the above-described Video Rental Store can trust the Pizza Parlor, because the Pizza Parlor is trusted, for example, by a well-known certificate authority. Such chaining of trust back to a basic trusted entity can include many levels.

[0075] Multi-tier trust also can be more restrictive and specific, so that entities are trusted conditionally to do specific things, for example, trusting an entity to issue specific rights. For example, in an exemplary embodiment, the Video Rental Store can have a subsidiary called the DVD Plaza, which the Video Rental Store allows to issue video club memberships.

[0076] Advantageously, the DVD Plaza can issue a customer a membership card including a legality expression specifying that the customer is a member of the Super Movie Watcher club and that the DVD Plaza can issue such club membership on behalf of the Video Rental Store. The customer then can go to the Pizza Parlor to receive the \$2 club discount. However, the relationship of the Pizza Parlor is with the Video Rental Store, not the DVD Plaza. The Pizza Parlor, however, can determine whether or not the DVD Plaza has the right to issue video club memberships by following the trust chain back to the Video Rental Store. Advantageously, the Pizza Parlor can determine that the Video Store, an entity the Pizza Parlor trusts, gave rights to issue memberships to the DVD Plaza, as specified in the card. Accordingly, the Pizza Parlor can authorize the customer to receive the \$2 discount.

[0077] By supporting multi-tier trust, advantageously, a card reader need not directly trust a party that makes a request in order to determine authorization, in order to use authentication data or in order to use any suitable other legality data. Nor does the reader need to directly know the issuer of a legality expression to accept or believe the legality expression. Advantageously, legality expressions issued by un-trusted entities can be verified using trust chaining to determine if the issuer had the right to issue the legality expressions. Since readers can be configured support multi-tier trust, advantageously, signed legality expressions can be issued with no need to update the knowledge base of the readers. Advantageously, even third parties can issue legality expressions that can be accepted by such readers.

[0078] Access control readers typically rely on authorization data that is kept in some knowledge base. The knowledge base can be used when determining whether or not an entity has access. In such systems, the knowledge base typically has to be updated each time permissions are given to some entity. Advantageously, the exemplary embodiments overcome such a problem, for example, by specifying such authorization data with a legality expression.

[0079] The exemplary embodiments, advantageously, provide support for offline environments by eliminating the dependency on contact with a separate entity, such as central system or a person, for example, to request or verify legality information, such as rights, contracts, and the like. For example, digitally signed legality expressions can be stored in a removable storage medium that can be presented to a suitable card reader, and the like. Advantageously, the card reader can be configured to include information regarding the trusted issuers, so the card reader can determine whether or not to trust a legality expression without a need to contact some other entity.

[0080] The exemplary embodiments, advantageously, provide relatively greater scalability and support for extensibility than, for example, bit encoding or other proprietary data representations. Additional legality information can be added to the removable storage medium, typically, without a need to modify hardware or software. For example, by employing an extensible Legality Expression Language, such as an XrML-based Legality Expression Language, and the like, advantageously, business specific extensions to the language can be added typically without a need for redesign or reconfiguration of the corresponding card reader systems. For example, the Video Rental Store can employ a legality expression to specify each type of club membership of a customer. In the case of digital coupons, a corresponding legality expression can be employed for each new type of coupon.

[0081] The exemplary embodiments, advantageously, provide an alternative mechanism to enable secured media, such as cards or keys, and the like. The media can include biometric information expressed in a Legality Expression Language, which can be used to authenticate an individual using the removable storage medium. For example, according to an exemplary embodiment, a device can be configured for digital signing, wherein the removable storage medium can be configured to authenticate a user via a fingerprint, iris, voice print, face print, and the like, information of the user included on the removable storage medium. If the user authentication fails on the device based on the removable storage medium, the digital signing on the device can be prevented.

[0082] In an exemplary embodiment, a removable storage device can be configured to perform self-authentication. For example, a passport or a license reader can be configured to read fingerprint information of a holder of the removable storage medium. If the reader determines that the read fingerprint matches fingerprint information specified with a legality expression stored on the removable storage device, the reader can be configured to presents authorization information to a border patrol agent, a police officer, and the like.

[0083] In an exemplary embodiment, a removable storage device can be configured to perform self-authorization. For example, a secure or trusted smart removable storage device can be configured to

store authorization information specified with a legality expression, such as information regarding areas within a building that the cardholder is authorized. The doors of the building can be configured to be equipped with a card reader device that authenticates the smart card and queries the smart card to determine if the cardholder is allowed to enter a given door. Since the smart card can be trusted and considered secure by the card reader, the query results provided by the smart card can be trusted. The smart card can be configured to interpret the legality expression to determine if the cardholder can be allowed to enter through the door. If the smart card determines that the cardholder is allowed to enter the door, the smart card can be configured to provide an appropriate response to the card reader, which can permit the cardholder entry.

[0084] The exemplary embodiments, advantageously, provide cascading of removable storage media, smart cards, and the like. For example, according to an exemplary embodiment, a will of a person can be written and associated, for example, with digital content, Internet services, and the like. The will can be cascaded and modified. The interpretation of the cascaded information can be context-based, for example, based on the order of cascaded information, devices, cards, and the like.

[0085] FIG. 2 illustrates an exemplary Legality Expression Management system 200 that can be implemented with one or more of the devices and subsystems of the Digital Rights Management System of FIG. 1. In FIG. 2, the exemplary Legality Expression Management system 200, for example, can include a removable storage device or medium 202, and a card reader and/or writer 204. The removable storage medium 202 can be configured as a repository or legality expression store 206 for storing one or more legality expressions, such as a contract 208, and a license 210. The card reader and/or writer 204 can be configured to read the expressions 206 or 208 from the removable storage medium 202 and can employ a Legality Expression Language interpreter component 212 to process the contract 208 and the license 210. The card reader and/or writer 204 also can be configured to write expressions onto the removable storage medium 202 and also can employ the interpreter 212 and optionally a validator 214 component to determine whether or not obligations or conditions specified in the legality expressions 208 and 210 have been satisfied.

[0086] The functionality of the reader and/or writer 204 can be included within one or more devices. The functionality of the interpreter 212 and/or the validation 214 components can be included within or separate from the reader and/or writer 204. The reader and/or writer 204 can use the interpreter 212, for example, to interpret any suitable information with a legal aspect or that can be used in a legal context and as specified in the contract 208. The removable storage medium 202 also can employ the interpreter 212 and the validation 214 components. The reader and/or writer 204 can employ a list or file 216 of one or more trusted issuers for determining trust relationships.

[0087] Exemplary information with a legal aspect or that can be used in a legal context and that can be expressed with a Legality Expression Language, for example, can include authentication information, such as credentials, or biometric information, such as fingerprints, iris scans, voice prints, and the like. Authorization information, for example, such as rights, obligation information, for example, such as fees to be paid, Official statements and results, for example, such as a confession, requests, for example, such as a letter from a landlord asking a tenant to pay additional fees for late rent, can be expressed with a Legality Expression Language.

[0088] The exemplary embodiments include secure removable storage media. Secure removable storage media, for example, can include media that can be used for signing, secure offline lending, secure transportation of electronic money (e-money) or electronic checks (e-checks), enforcement of restraining orders, enforcement of probation rules, enforcement of contracts, Digital Rights Management for content, such as music, through altering at distribution or restoration at consumption, and the like.

[0089] In addition, the exemplary embodiments include removable storage media and smart cards that can be cascaded together. For example, according to an exemplary embodiment, a will of a person can be written and associated, for example, with digital content, Internet services, and the like. The will can be cascaded and modified. The interpretation of the cascaded information can be context-based, for example, based on the order of cascaded information, devices, cards, and the like.

[0090] The exemplary embodiments include, for example, the removable storage medium 202 that can be used to store the legality 208 and 210 expressions written in an Expression Language. Exemplary removable storage medium 202, for example, can include or be included in memory hardware or devices, such as memory cards or smart cards, dumb cards, such as credit cards, any suitable type of disks, such floppy disks, hard disks, optical disks, Compact Disks (CDs), Digital Versatile Discs (DVDs), remote control devices, chip-based devices, key-based devices, cellular phones, pagers, handheld devices, palmtop devices, Internet appliances, desktop computers, laptop computers, Personal Digital Assistants (PDAs), game consoles, music players, and the like.

[0091] The removable storage medium 202 can employ the reader and/or writer 204 components, and can employ the interpreter 212 and validation 214 components, for example, to determine whether or not conditions or legal obligations are met, and can use the list 216 of trusted issuers, for example, for determining trust relationships. In addition, the removable storage medium 202 can be configured to detect possible conflicts with the legality 208 or 210 expressions that are stored on the removable storage medium 202. For example, the removable storage medium 202 can be configured to detect whether or not one contract or license conflicts with another contract or license. The removable storage medium 202 need not be secure, and the removable storage medium 202 need not be a trusted repository of the legality expressions.

[0092] The reader component of the reader/writer device 204 can be configured to read the legality 208 and 210 expressions from the removable storage medium 202 and employ the interpreter 212. The reader component also can employ the validator 214 to determine whether or not conditions or legal obligations specified in the legality 208 and/or 210 expressions can be met, and can employ the list 216 of trusted issuers. The various types of removable storage media 202 of the exemplary embodiments can include a corresponding reader component, for example, such a card reader used on a game console, music player, and the like.

[0093] The writer component of the reader/writer device 204 can be configured to write legality expressions on the removable storage medium 202. The writer component can include a legality expression generator, and can be configured to receive expressions from an outside source, such as over the Internet or over an intranet. The writer component also can employ the interpreter 212 and the validator 212 to determine whether or not conditions or legal obligations specified in the legality 208 and/or 210 expressions can be met, for example, before writing data to the removable storage medium 202 and also can employ the list 216 of trusted. Exemplary reader and/or writer components, for example, can include remote control devices, chip-based devices, key-based devices, cellular phones, pagers, handheld devices, palmtop devices, Internet appliances, desktop computers, laptop computers, PDAs, game consoles, music players, and the like.

[0094] In an exemplary embodiment, the components of the system 200 can employ the interpreter 212 and/or the validator 214, for example, to perform authentication, authorization, resolution of legality matters, enforcement of conditions and/or legal obligations based on the legality 208 and/or 210 expressions. In an exemplary embodiment, the interpreter 212, for example, can be employed to interpret any suitable information with a legal aspect or that can be used in some legal context, and the like. In a further exemplary embodiment, the removable storage media 202 also can be configured to perform such processes.

[0095] In addition to authenticating users of the removable storage media 202, the devices of the Legality Expression Language system 200 can perform authentication of other devices in the system. For example, a card reader can authenticate the card being presented to verify that the card is not counterfeit. In addition, the devices can seek authorization to function with other devices in the system 200. Advantageously, such authorization can be specified in the legality 208 or 210 expressions. For example, the system 200 can be configured so that the removable storage medium 204 can be used once a day, in a specific context, and the like. Advantageously, the exemplary embodiments enable numerous authentication and authorization models.

[0096] FIG. 3 is a flowchart for illustrating an exemplary process of trust chaining that can be employed in the systems of FIGS. 1 and 2-10. In an exemplary embodiment, the list 216 of trusted issuers, advantageously, can be employed to determine entities whose expressions, for example, such as the expressions embodied in the contract 208 and the license 210, can be trusted. Such entities can be used to form a root level of trust used during the trust chaining process. Advantageously, the exemplary trust chaining process can be employed for determining whether or not a legality expression, for example, digitally signed by an unknown party can be trusted.

[0097] Accordingly, in FIG. 3, at step 302, an expression, such as the legality expression in the form of the license 208 or 210, can be obtained and an issuer can be extracted from the obtained expression. At step 306, it is determined whether or not an issuer extracted from the expression can be found on the list 216 of trusted issuers. If at step 306 it cannot be determined that the issuer can be trusted, at step 308, another expression that allowed the issuer to issue the expression currently being processed is searched for and if such an expression can be found, as determined at step 310, control returns to step 304 for processing of the found expression.

[0098] The processing of step 304-310 can be repeated until a trusted issuer can be found, in which case, at step 314, a true result indicating that the original expression can be trusted as being from a trusted issuer can be returned. Otherwise, at step 312, a false result indicating that the original expression cannot be trusted as not being from a trusted issuer can be returned. The exemplary trust chaining process of FIG. 3 can be repeated for processing of further expressions.

[0099] In an exemplary embodiment, the devices and components of the Legality Expression Management system 200, advantageously, can be programmable to enable users to change the way that the components behave. For example, the removable storage medium 202 can be programmed to not accept expressions determined, for example, to be spam, illegitimate, unreliable, and the like.

[0100] Advantageously, the exemplary embodiments can be protected by and/or incorporated into the Digital Rights Management system of FIG. 1. Any suitable device or subcomponent of the Legality expression management system 200 can be Digital Rights Management-enabled so that parties with specified rights or obligations can use such a device or subcomponent. In an exemplary embodiment, the removable storage medium 202 can be used to store biometric characteristics corresponding to the owner of the removable storage medium 202. Advantageously, an individual that is determined to match such characteristics then can use the removable storage medium 202, for example, as a signing key, and the like.

[0101] In addition, various restrictions can be placed on use of the removable storage medium 202, for example, such as exercise limits and validity intervals, prerequisite rights, parameters, such as temperature, security of the environment, any suitable environment variable, and the like.

[0102] FIG. 4 illustrates an exemplary embodiment of the Legality Expression Management system of

FIG. 2. In FIG. 4, the exemplary system 400, for example, can include a reader/writer device 404 having expression interpretation 412 and validation 414 components and a removable storage device 402. The reader/writer 404 can communicate with a list 416 of trusted issuers. The removable storage device 402 can include an expressions store 406 for storing a contract 408 and a license 410.

[0103] As shown in FIG. 4, the contract 408, for example, can be used to specify one or more obligations and a witness to the contract 408. The license 410, for example, can be used specify one or more grants and an issuer of the license 410. The interpreter 412 and the validator 414 components can read the contract 408 and the license 410 from the expressions store 406 and interpret and validate expressions from the contract 408 and the license 410. The witness and the issuer can be verified by the interpreter 412 and the validator 414 components based on the list 416 of trusted issuers.

[0104] FIG. 5 illustrates an exemplary embodiment of the Legality Expression Management system of FIG. 2. In FIG. 5, the exemplary system 500, for example, can include a card 502 that can serve as a license and contracts store 506, a card reader device 504 having expression authorization 522 and authentication 524 components that can communicate with an interpreter 512.

[0105] As shown in FIG. 5, the license and contracts store 506 can be used to store a license 510, for example, that can be used to specify an issuer of the license 510 and biometric information, such as a thumbprint, and the like, of the card 502 holder. The issuer specified in the license 510 can be verified by the authorization component 522 based on a list 516 of trusted issuers. Advantageously, the system 500, for example, can be employed for providing secured access control based on the biometric information.

[0106] FIG. 6 illustrates an exemplary embodiment of the Legality Expression Management system of FIG. 2. In FIG. 6, the exemplary system 600, for example, can include a card 602 that can serve as a license and contracts store 606, a card writer 604 having an expression generation 630 component and expression authorization 622 and authentication 624 components that can communicate with an expression interpretation 612 component.

[0107] As shown in FIG. 6, the license and contracts store 606 can be used to store licenses 610 and 618. The license 610, for example, issued by a video game manufacturer, can be used to specify a grant to play a video game, and the like. Similarly, the license 610, for example, issued by a video store, can be used to specify a grant to play a movie, and the like. The expression generator 630 component can be used to write legality expressions in the form of a license or a contract onto the license and contracts store 606 of the card 602. The authorization 602 component can be used to authorize the licenses 610 and 618 after being interpreted by the interpreter 612 based on the list 616 of trusted issuers. Similarly, the authentication 624 component can be used to authenticate the licenses 610 and 618 after being interpreted by the interpreter 612. The issuers specified in the licenses 610 and 618 can be verified by the authorization component 622 based on a list 616 of trusted issuers. Advantageously, the system 600, for example, can be employed for providing secured access control and license or contract generation for movies, video games, music, and the like.

[0108] In an exemplary embodiment, validating or authenticating a legality expression can include determining whether or not the expression has been tampered with, but also can include validating one or more conditions that can result from the interpretation of the expression and possibly making a choice of which conditions or conditions to employ. For example, via suitable legality expressions, a first video store can issue a right to play a movie to a customer on the condition of payment of a \$3 fee and a second video store can issue the right to play the movie to the customer on a condition that personal information of the customer is provided to a Web service of the second video store.

[0109] Then, when the customer takes a license card including licenses corresponding to the above offers, for example, to an on-demand media player, the media player can be configured determine that the customer can play the movie by either paying the \$3 fee to the first video store or by sending the personal information of the customer to the Web service of the second video store. In a further exemplary embodiment, the media player may not provide an option to the customer, but rather can select one of the options for the customer in a dumb or smart way. If a selection is made to pay \$3 fee to watch the movie, for example, a condition validator on the media player can be configured ensure that the \$3 fee is paid before letting the media player play the movie.

[0110] In an exemplary embodiment, during authentication and authorization, a card reader and/or writer, such as the card reader and writers 204 and 404, the card reader 504, and the card writer 604, can authenticate the removable storage medium and/or an owner of the removable storage medium, such as the removable storage devices 202 and 402, and the cards 502 and 602. Advantageously, credentials that can be employed for such an authentication process can be specified using a legality expression, such as the contracts 208, and 408, and/or the licenses 210, 410, 510, 610, and 618.

[0111] In an exemplary embodiment, during the authentication, the reader and/or writer can read credentials expressed using a legality expression from the removable storage medium. Advantageously, such credentials also can be linked to or include biometric information corresponding to a holder of the removable storage medium. For example, a Read Only Memory (ROM) area of a card, such as the cards 502 and 602, can include license information of a driver and also store a map of the face of the driver for biometric facial recognition purposes. Advantageously, only an individual corresponding to the identified face map can use such a card. Such biometric information, advantageously, can be stored using a legality expression, for example, expressed as follows:

2 Grant Principal (facial geometry: Can be a JPEG) PossessProperty ThisCard (id=123456789) /Grant

[0112] An authentication component, such as the authentication components 524 and 624, advantageously, can review such credentials and provide an authentication result, such as a "yes" or "no" result and optionally a further credential or credentials. After performing the authentication process, the reader and/or the writer, such as the card reader and writers 204 and 404, the card reader 504, and the card writer 604, can perform an authorization process, for example, using a legality expression, such as the contracts 208, and 408, and/or the licenses 210, 410, 510, 610, and 618, associated with an issuer thereof, using the removable storage medium, using a reader or writer cache, using a local storage device, using a centralized or semi-centralized expression repository, a combination thereof, and the like. The authorization process, for example, can include checking whether or not the authenticated entity can be authorized to perform a particular action, use a particular resource, and the like. In an exemplary embodiment, the reader and/or writer, for example, can function independently, in conjunction with a central controller (not shown), and the like.

[0113] The authorization components, such as the authorization components 522 and 622, of the reader and/or writer, such as the card reader 504 and the card writer 604, for example, can employ a set of issuers that represent root trust, such as issuers whose statements can be trusted blindly, and the like. Advantageously, issuers unknown to the reader and/or writer can issue legality expressions that the reader and/or writer and/or the central controller can trust, if a chain of trust leads back to one of the root trusted issuers, for example, as specified in a list of trusted issuers, such as the lists 216, 416, 516, and 616 of trusted issuers.

[0114] Advantageously, the reader and/or writer can be configured to operate online when the central controller can be reached and offline when the central controller cannot be reached. The central controller can be configured to store trusted issuer information that can be synchronized with the

authorization components, such as the authorization components 522 and 622, of the reader and/or writer, such as the card reader 504 and the card writer 604. In addition, the reader and/or writer can be configured to cache authentication and authorization information during periods when the central controller is unreachable and provide such information when the central controller becomes accessible. In an exemplary embodiment, the authorization information, for example, also can include information regarding who can use the removable storage device, how the removable storage device can be used, when the removable storage device can be used, and the like.

[0115] FIG. 7 illustrates an exemplary embodiment of the Legality Expression Management system 200 of FIG. 2 for providing access control. In FIG. 7, the exemplary system 700, for example, includes a card reader 704 having expression authorization 722 and authentication 724 components, wherein each of the authorization 722 and the authentication 724 components can include respective expression interpretation 712 and 720 components. In the exemplary access control embodiment, a user can be issued a badge in the form of a card 702 having an expressions store 706 and that the user can present to gain access, for example, to parts of a workplace of the user in a building called Corporate Towers.

[0116] In an exemplary embodiment, when the user arrives at the workplace, the user, for example, can place the badge close to or in a badge reader, such as the card reader 704, provided at a door that the user wishes to open. In an exemplary embodiment, Security personnel of the Corporate Towers can be trusted issuers representing a root trust, for example, as specified in a list 716 of trusted issuers.

[0117] Advantageously, the card reader 704 can be configured to trust statements, for example, legality expressions, such as the license 710, generated and/or issued by the Security personnel of the Corporate Towers. If an individual tries to open a door of the Corporate Towers using a card having a license issued by the Corporate Towers and specifying that the cardholder has the right to open the door at suitable times, the authorization 722 component can be configured to allow such an individual access to enter the corresponding door.

[0118] In an exemplary embodiment, the Corporate Towers can allow a Company to issue access rights to open doors on the 14th floor leased by the Company from the Corporate Towers, for example, as specified in the license 710. For example, the Company can issue the card 702 to a visitor that can include the license 718 stored in the expressions store 706 of the card 702 and granting the visitor access to a main door to a suite of the Company on the 14th floor of Corporate Towers during the first week of October 2002. Advantageously, the legality expression corresponding to the license 718 can be signed by the Corporate Towers to allow verification that the Company was allowed to issue the license 718.

[0119] For example, on October 1 the visitor presents the card 702 to the card reader 704 at the main door of the Company suite. The card reader 704 using the interpreter 720 of the authentication 724 component then can authenticate the visitor as the principal based on the license 718. The authorization 722 component of the card reader 704 then can employ the interpreter 712 to check the license 718 on the card 702 based on the list 716 of trusted issuers to determine whether or not the visitor can be authenticated and has the right to open the door to the suite of the Company. During the interpretation process, the authorization 722 component can determine if the license 718 was signed by the Company for allowing the visitor to open the door to the suite of the Company. If, however, the authorization 722 component determines that the license 718 was not issued by a trusted principal, such that there is no root trust for the Company, access to the door of the suite of the Company can be denied.

[0120] Advantageously, the authorization 722 component of the card reader 704 can verify whether or not the Company has the right to issue the license 718. For example, the interpreter 712 can determine from the license 710 that the license 710 was signed by the Corporate Towers and grants the Company the right to issue the license 718. Advantageously, since the Corporate Towers can be specified as a

trusted issuer in the list 716 of trusted issuers, no further evidence need be employed in the authorization process.

[0121] The authorization 722 component also can be employed to determine whether or not conditions specified by the Company are met, such as the ValidityInterval and EntryThrough conditions specified in the license 718, before opening the door to the suite of the Company. However, since the visitor presented the card 702 on October 1 and the visitor is trying to open the main door to the Company suite, the visitor can be allowed entry based on the license 718.

[0122] The present invention include recognition that as the Internet continues to gain momentum as a favorite research tool, more and more stores and manufacturers can begin to post and offer coupons on the Internet. According to exemplary embodiments, coupon offers can be expressed digitally or electronically using a rights and/or legality expression, for example, such as expressions based on XrML. Advantageously, the exemplary embodiments, for example, can be employed to enable the electronic redemption of such digital coupons at physical stores.

[0123] For example, an individual or group of individuals can collect digital coupons on a card or other removable storage medium, such as the removable storage devices 202 and 402, and the cards 502, 602 and 702, selectively or by an automated process, and the like. In an exemplary embodiment, the digital coupons can be downloaded from the Internet or any suitable location and can be stored onto such a card or removable storage medium. Stores also can download digital coupons onto the cards of customers and that can be used on present or future visits to such stores or in other stores that can accept such digital coupons.

[0124] In an exemplary embodiment, during check out, customer can present a card, such as the cards 502, and 702, to a reader, such as the card readers 504 and 704, at a checkout register of the store. Advantageously, the cardholder can be authenticated using authentication components, such as the authentication components 524 and 724, and the card reader can be configured to retrieve respective digital coupons from the card corresponding to items being purchased. Advantageously, the coupons also can be verified, for example, using authorization components, such as the authorization components 522 and 722. In an exemplary embodiment, such verification can include checking the authenticity of the digital coupons, determining whether or not each digital coupon was issued by an entity trusted or accepted by the store, and the like.

[0125] Based on the exemplary access control process, the store need not directly trust the digital coupon issuer to accept the digital coupon. For example, the store can be configured to accept coupons verified via trust chaining to be issued by business partners of the store, business partners of the business partners of the store, competitors of the store, and the like. Advantageously, such a mechanism, for example, can be employed to allow the store to lower prices, to beat a prices of a competitor, and the like.

[0126] In an exemplary embodiment, if several coupons having different conditions apply to a same item that is being purchased, the card reader can be configured to request input from the customer as to which coupon to use, automatically determine which coupon to use, and the like. The selected coupons then can be applied to the purchase.

[0127] In a further exemplary embodiment, during checkout, additional coupons can be applied to the purchase, additional coupons can be download to the card of the customer, and the like. For example, two coupons can be added to the card, wherein one coupon entitles the customer to a 20% discount on a next purchase and another coupon entitles the customer to not have to pay taxes on purchases over \$50. After the coupon processing has been completed, the customer can pay for the purchased items less the

applied discounts and leave the store. Advantageously, at some later time, the customer can return the store and, for example, purchase \$100 worth of items, such as groceries, and present the card to the card reader during checkout to receive the 20% and the no tax discounts, thus, only paying \$80 for the items.

[0128] In an exemplary embodiment, a legality expression can be employed to specify an issuance of right, wherein such issuance need not entail consent of the parties involved. For example, a store can issue a right in the form of a digitally signed coupon specified with a legality expression over the Internet to a consumer without the consent of the consumer. The consumer then can make a decision as whether or not to use the coupon. The coupon can be downloaded onto a removable storage device of the consumer and then can be taken to the store by the consumer. A coupon reader at the checkout register can include an expression interpreter, such as an XrML interpreter, and the like. Advantageously, such a coupon can be employed to provide discounts on non-digital items, such as consumer goods, appliance, services, and the like.

[0129] In exemplary embodiment, in manner similar to that described above with respect to coupons, transportation of digital tickets can be handled and employed, advantageously, for non-digital goods. Digital tickets are further described in commonly assigned U.S. Pat. No. 6,236,971 to Stefic, et al., entitled "System for Controlling the Distribution and Use of Digital Works Using Digital Tickets," the entire disclosure of which is hereby incorporated by reference herein.

[0130] FIG. 8 illustrates an exemplary embodiment of the Legality Expression Management system of FIG. 2. In FIG. 8, the exemplary system 800, for example, can include a game console 826 having an expressions storage 828 component and a card reader/writer device 804 having expression authorization 822 and authentication 824 components that can communicate with an expression interpretation 812 component.

[0131] The game console 826 can be configured to allow users to play one or more games, for example, if the users have respective licenses for the games, such as the licenses 810 and 818. The licenses 810 and 818 in the form of a legality expression for the games can be stored on a card, key card, and the like, such as the card 802 having a license and contracts store 806.

[0132] Advantageously, the games can be played on any suitable game console 826, if the key card 802 with the licenses 810 and 818 to play the games is inserted into that game console 826. In an exemplary embodiment, the game consoles 826 can be configured such that users can play the games on different game consoles 826, but only on one game console 826 at a time. Advantageously, the games produced for the game console 826 need not have any suitable Digital Rights Management directly associated with the games, such that the games can be configured as clear content with no special restrictions associated with the games.

[0133] In an exemplary embodiment, the users can purchase the licenses 810 and 818 for the games from physical stores, over the Internet, and the like. Advantageously, the game console 826, for example, can be configured to connect to the Internet over a communications network 870 to purchase licenses for a game or a set of games, for example, from a game store 832, a toy store 834, a video store 836, and online game store 838, and the like.

[0134] The digital licenses 810 and 818, for example, can be securely transferred onto the key card 802, the game console 826, onto some other trusted device, and the like. Advantageously, users can lend each other games by securely lending the corresponding licenses to one another. At the same time, the games can be usable on the console 826 that has the corresponding license. For example, if a first user lends a game license to second user, the second user can use the game on the game console 826 of the second user, but the first user cannot use the game on the game console 826 of the first user until the second

user returns the license. Advantageously, the licenses 810 and 818 can be moved around between trusted devices, as specified in the corresponding legality expression.

[0135] The exemplary systems and methods can be applied to various other businesses, for example, businesses related to music, movies, and the like, as will be appreciated by those skilled in the relevant art(s). Advantageously, any suitable user device can take advantage of the exemplary embodiments. In addition, the exemplary embodiments can be applied to any suitable type of content, such as movies, music, services, and the like.

[0136] Advantageously, the exemplary embodiments provide secure transfer of digital licenses and/or contracts between trusted devices. A portable device can be used to transport a digital license or contract from one device to another. Depending on the rights granted or the obligations imposed, a license or contract can be transferred permanently, for example, removed from the transferring device and placed on the receiving device, copied, re-issued with new conditions or obligations, shared using a state mechanism, and the like.

[0137] In an exemplary embodiment, an e-money system using trusted removable storage medium, such as the card 802, for example, can be employed to securely transfer and carry e-money. A trusted system can be employed to securely interact with the trusted removable storage medium during transfers of the e-money. Such secure interaction can be performed in a manner similar to the lending of the digital licenses 810 and 818. In exemplary embodiment, e-money cards can be configured to be widely accepted and the e-money can be based on a standardized Legality Expression Language.

[0138] In an exemplary embodiment, a digital copy of a dollar bill can be configured as an e-dollar, and the trusted system can be configured to protect against illegal activities, such as hacking, counterfeiting, and the like, advantageously, preventing the spread of counterfeit e-money. In an exemplary embodiment, users can download the e-money over the Internet, receive the e-money through e-mail, acquire the e-money through some other means, and the like. Once acquired, the user can store the e-money on the removable storage medium, such as the card 802, and the like, and the user then can take the card to a bank or some other entity to spend or to cash out the card.

[0139] An electronic check (e-check), an electronic-checkbook (e-checkbook), and the like, also can be configured on such a removable storage medium, advantageously, allowing for the creating and signing of electronic checks. The removable storage medium can authenticate the user by various means, for example, using biometrics, such as a fingerprint scan, iris scan, and the like.

[0140] In an exemplary embodiment, credit authorizations also can be carried on a suitably configured removable storage medium. For example, a credit card company can be configured to issue a legality expression in the form of a certificate specifying that a user has a specific account and that the user can use the account as a credit line, for example, subject to a state reference check.

[0141] In an exemplary embodiment, video arcades can be configured to store video game credits on cards, such as the card 802, and change or token machines can be configured to accept money and place the corresponding video game credits on the card. Advantageously, the user can insert the card into a video arcade game machine to play the corresponding game and the fee for playing the game can be automatically deducted by the game machine from the card of the user. In an exemplary embodiment, the video arcade game cards can be configured so as to be limited to a specific video arcade, for example, using a corresponding authorization component, interpreter, and list of trusted issuers, such as the authorization component 822, the interpreter 812, and the list 816 of trusted issuers.

[0142] In an exemplary embodiment, a digital driver's license can be expressed using a legality

expression, such as the license 510, stored on a removable storage medium, for example, on a card, such as the card 502, and the like. Advantageously, biometric information specified in the legality expression can be used to verify the identity of the holder of the digital driver's license card. The biometric information included in the digital driver's license card, for example, can include facial geometry information, fingerprint information, iris pattern information, and the like, of the holder of the digital driver's license. The biometric information can be stored on a secure area of the card, such as a ROM area, and used to automatically authenticate the holder of the card using an electronic card reader device, such as the card reader 504. The card reader device, for example, also can be configured to display, present, and the like, the biometric information specified in the card for verification by a human.

[0143] In an exemplary embodiment, a card can be configured to include authorization information that grants an authenticated person certain rights or that specifies duties or obligations of such a person. Such cards, for example, can be configured to specify information regarding restraining orders that have been filed against individuals and can be configured to list places that such individuals can or cannot go. For example, such cards can be configured such that people on probation are not allowed into bars. In an exemplary embodiment, a trusted system can be configured to securely modify the information on such a card and employ signed legality expressions.

[0144] In exemplary embodiment, a digital driver's license in the form of a smart card or a smart removable storage medium can be used to authenticate an individual, for example, by allowing scanning of a fingerprint or other biometric data of the individual. Advantageously, with the exemplary embodiment, digital driver's licenses can be configured so as to be self-contained and not entail additional devices to authenticate an individual. For example, once the smart card has been used to authenticate the license holder, the card can be configured to allow or to force the license holder to use or present to some entity the rights and/or legality expressions within the card associated with the license holder. Advantageously, the exemplary embodiments can be applied to applications other than driver's licenses, as will be appreciated by those skilled in the relevant art(s).

[0145] In an exemplary embodiment, a smart card or smart removable storage device, and the like, advantageously, can be employed as a key for allowing electronic or digital signing. For example, the removable storage device can be configured to include biometric information expressed in a legality expression stored in a secure area of the removable storage device, such as in a ROM area, and the like, of the device. The right to sign with a specific signature can be included within a legality expression that can be signed by a widely trusted and accepted entity and stored within the device. Corresponding reader and writer devices can be configured to either trust the removable storage device or can be configured to use legality expressions provided in the removable storage device to determine whether or not to trust the holder of the device and to determine which signature to use when the holder wishes to digitally sign something using the removable storage device.

[0146] The reader or writer device can be configured to authenticate the holder by scanning the fingerprint or other biometric data of the holder and comparing the scanned data with the biometric information stored within the removable storage device. If such authentication fails, the reader or writer device can be configured to prevent the removable storage device from being used for digital signing. The removable storage device also can be configured so as to be restricted from being used for signing certain transactions, for example, based on a legality expressions stored therein. For example, the removable storage device can be configured to include a legality expression in the form of a contract that specifies that the removable storage device cannot be used for digitally signing a document that relates to a real estate transaction, and the like.

[0147] In an exemplary embodiment, a removable storage medium, for example, can be configured to store legality expressions that can be used to specify the behavior of a software or hardware system

and/or component. For example, such a legality expressions can be in the form of specified policies that the component or system can follow. Advantageously, a given behavior can be transported from one device or software component to another or behavior in one environment can be used in another environment.

[0148] For example, the behavior of one robot can be transferred to another robot, the behavior of one security system can be transferred to another, settings of one computer of a user can be transferred to every computer of the user, and the like. Advantageously, a person that frequently uses different computers, such as public computers in places like Internet cafes, and the like, can find the latter capability quite useful. In an exemplary embodiment, a legality expression can be employed to specify any suitable type of relationship between software or hardware components or devices.

[0149] FIG. 9 illustrates an exemplary embodiment of the Legality Expression Management system of FIG. 2. In FIG. 9, the exemplary system 900, for example, can include a smart removable storage device 902 serving as an expressions store 906, and a reader/writer device 904 having expression interpretation 912 and validation 914 components. The exemplary system 900, advantageously, can be employed as a vehicle access and usage control system. A vehicle, such as a car, a bus, a truck, and the like, can be configured to include the reader/writer device 904 that can include authorization and authentication components within the validator 914 and that can communicate with the interpreter 912.

[0150] In an exemplary embodiment, the smart removable storage device 902 can be configured as the key to the vehicle and can be programmed to carry a legality expression specifying that the owner of the vehicle is allowed to open the vehicle, use predetermined features of the vehicle, start the vehicle, and the like. A digital driver's license of the driver of the vehicle can be configured to include a legality expression in the form of a contract 908, for example, specifying the information for the driver, and any restrictions and/or obligations imposed on the driver, for example, by a Judge of a court having jurisdiction over the driver and which can be verified by a list 916 of trusted issuers. The driver can insert the digital driver's license into the card reader/writer device 904, and the authentication and authorization components of the validator 914 can employ the interpreter 912 to determine the identity of the driver and whether or not the identified driver has the right to drive the vehicle. Advantageously, the vehicle can be configured to include a Global Positioning System (GPS), for example, that can be employed to prevent the driver from driving outside of an area specified in the contract 908.

[0151] In an exemplary embodiment, a legality expression need not be enforced. For example, the legality expression can be used to specify a receipt or a confession that need not be enforced. In a court, for example, evidence in the form of a legality expression can be presented. In addition, a legality expression need not specify an obligation, for example, when a receipt or confession in the form of a legality expression is presented as proof. Advantageously, the court can employ a suitable reader device, for example, including an expression interpreter, that can be configured to extract semantics information from evidence in the form of a legality expression and present the extracted meaning of the evidence to a judge or jury of the court.

[0152] In an exemplary embodiment, smart removable storage media, advantageously, can be employed to enforce restraining orders, probation rules, contracts, and the like. Advantageously, a legality expression can be configured to specify where an individual can or cannot go, what a person can or cannot do, and the like. In an exemplary embodiment, the removable storage device 902 can be configured to enforce the legality expressions, such as contracts, licenses, and the like, and/or the reader/writer device 904 can be configured to enforce expressions stored within the removable storage device 902. For example, the exemplary system 900 can be configured such that when an individual leaves some predetermined boundary specified in the contract 908, the individual can be shocked by a electronic shocking device (not shown) included within the reader/writer 904 or the vehicle, the vehicle

can be automatically disabled, the authorities can be notified of the violation, and the like.

[0153] In an exemplary embodiment, the sharing of legality or rights data among businesses, such as the Video Rental Store and the Pizza Parlor, advantageously, can be provided. For example, the problems associated with the interoperation of multiple businesses, such as problems relating to extending legality or rights constructs without a need to reconfigure reader and writer devices, problems relating to scalability issues, problems relating to support for offline solutions, and the like, advantageously, can be addressed.

[0154] In an exemplary embodiment, the removable storage media and the legality expressions can be configured based on industry standards. For example, the Video Rental Store and the Pizza Parlor can adopt such standards and begin developing business relationships based thereon.

[0155] In exemplary embodiment, the Video Rental Store can be configured to provide several membership types, such as the Super Movie Watcher club, the Movie a Week Club, and the like. The members of the Video Rental Store can receive a generic membership card onto which the Video Rental Store can download legality expressions specify such membership types. Each member can have several membership types, and the legality expression can be created and downloaded for each membership type of a given customer onto a respective card. For example, when a customer rents a movie, the card of the customer can be scanned to identify the customer and the membership types of the customer. Advantageously, the price that the customer pays for a movie rental can be based on the membership type as specified by the legality expression.

[0156] The Pizza Parlor can be configured to give a \$2 discount to members of the Super Movie Watcher club of the Video Rental Store. The Pizza Parlor can scan the card of the customer for a legality expression digitally signed by the Video Rental Store and specifying that the customer is a member of the Super Movie Watcher club. Advantageously, since the legality expressions can be signed, the Pizza Parlor need not contact the Video Rental Store to verify a membership type of a given customer. In addition, since the Video Rental Store and the Pizza Parlor can employ the standardized expression language and removable storage medium, the Video Rental Store and the Pizza Parlor, advantageously, can share the legality or rights information specified on the cards of customers brought from one business to the other.

[0157] Advantageously, by employing the legality expressions, for example, based on XrML, the Video Rental Store and the Pizza Parlor can add legality expressions to cards of customers without a need to redesign or reconfigure card reader and writer devices. In addition, the Pizza Parlor and the Video Rental Store can add customized language extensions to the legality expressions without a need to modify the card reader and writer devices. Advantageously, as the Pizza Parlor develops other business relationships with other businesses, the Pizza Parlor can use a similar infrastructure to enhance business relationships with such other businesses.

[0158] The exemplary embodiments can be applied to various other businesses, applications, and the like, as will be appreciated by those skilled in the relevant art(s). Advantageously, a removable storage medium can be configured to store corresponding legality expressions for a given entity, applications, or business type. In an exemplary embodiment, such legality expressions can be obtained through independent or dependant associations with many different parties, such as the Department of Motor Vehicles (DMV), the police, employers, stores, courts, people, and the like. By employing a standardized Expression Language to express the legality or rights data, the various different parties can securely use the legality or rights data of one another, advantageously, using the same type of removable storage media and reader and writer devices.

[0159] In an exemplary embodiment, the Digital Rights Management system 100 of FIG. 1 can be configured to employ the legality expressions, the removable storage medium, and the reader and writer devices of FIGS. 2 and 4-10, for example, to identify users desiring access to resources protected by the Digital Rights Management system 100. Advantageously, the removable storage medium can be configured as a digital driver's license or some other form of identification that the Digital Rights Management system 100 can employ during the authentication process. The removable storage medium also can include authorization information, such as legality expressions that grant the owner of the removable storage medium rights to the protected resource.

[0160] In an exemplary embodiment, the removable storage media can be employed to process legality expressions efficiently. For example, after validating a legality expression, a legality expression preprocessor can be configured to deploy the expressions, for example, to different search spaces, based on predetermined criteria, and the like. The criteria can be extracted or determined from the legality expression, or the criteria can be provided to the preprocessor in addition to the legality expression. The legality expressions can be partitioned over different removable storage media, for example, with a defined order or priority assigned to each of the legality expressions, advantageously, providing relatively faster results on common search queries.

[0161] For example, in an exemplary embodiment, a county clerk system can be configured to sort legality expressions based on type, wherein wills go into one removable storage medium, birth records go into another, restraining orders can be placed in another, and the like. The legality expressions also can be sorted into different removable storage media, for example, based on dates thereof. The removable storage media holding the most recent expressions can be given a relatively higher priority. The removable storage media including expressions more than a specified number of years old can be removed, so that the query system need not process such expressions during search requests. The older data can be moved to other systems or can be archived. In addition, the removable storage medium, for example, can be configured to perform smart processing of the legality expressions.

[0162] In an exemplary embodiment, Digital Rights Management of content, such as music, movies, and the like, advantageously, can be provided based on the exemplary systems of FIGS. 1, 2 and 4-10. For example, a music distributor can be configured to produce Digital Rights Management-enabled content in which music files sold can be distorted, for example, by altering the sound waves of the music. In order to listen to a corresponding music file, the user can employ a removable storage medium having a legality expression in the form of a license to allowing the restoring and the playing of the music file. In an exemplary embodiment, the user then can take the removable storage medium to a music store or to another suitable place to download the licenses onto the removable storage media. In a further exemplary embodiment, an employed music restoration device can be configured to connect to the Internet to obtain the music licenses therefrom.

[0163] The restoration device, advantageously, can be configured to work in conjunction with a music player. For example, if a corresponding license is presented for the music that is being played, the restoration device can be configured to take the output of the music player and convert the output music back to an original unaltered form for listening. The exemplary sound wave modifications, for example, can include changing amplitude of the sound signals, filtering of the sound signals in the temporal domain, adding a noise signal to the sound signal in the temporal domain, filtering the sound signal in the frequency domain, adding extra signals to the sound signal in the frequency domain, convolution of the sound signal with a known variable signal, switching of the sound signal in one or more parts of the frequency spectrum, selecting a variable frequency for the sound signal, and the like.

[0164] FIG. 10 illustrates an exemplary embodiment for cascading of removable storage medium and/or smart card devices and that can be employed in the systems of FIGS. 1 and 2-9. In FIG. 10, the

removable storage media or smart card devices, advantageously, can be cascaded together, for example, to fully take advantage of the capabilities of the devices. The devices can be cascaded using any suitable arrangement, such as a series arrangement, a parallel arrangement, a ring arrangement, a star arrangement, other geometric arrangements, any suitable combination thereof, and the like. The devices can be connected to a central or main unit (not shown) or can be configured so as to be stand-alone devices.

[0165] Advantageously, cascading can provide relatively more flexibility, combinations, and possibilities for mixing the devices and subcomponents of the exemplary systems of FIGS. 1 and 2-9. For example, cascading can be employed to provide a relatively economical way to address a wider variety of potential applications. In addition, a common standard can be established, and various manufacturers can contribute to the development of compatible subcomponents and devices. Each subcomponent and device can be configured to be function-specific in terms of hardware and software, advantageously, making the subcomponent or device relatively smaller, cheaper, and faster.

[0166] In FIG. 10, for example, five removable storage devices (S1-S5) 1080-1088, such as the storage device 202, can be cascaded together, wherein the devices 1080 and 1082 can be cascaded in series as a first unit (U1) 1090, and the devices 1084, 1086, and 1088 can be cascaded in series as a second unit (U2) 1092. In addition, the units U1 and U2 can be configured in a parallel configuration.

[0167] In an exemplary embodiment, the removable storage devices S1 and S2 can be configured to store redundant information, for example, for enabling secure data storage, or can be configured to store complementary information. Advantageously, the removable storage devices S1 and S2 in such as complementary configuration can be employed for security purposes by making it harder for a potential hacker to access the all of data in one place and at one time.

[0168] In an exemplary embodiment, the removable storage devices S1 and S2 can be configured so as to be used for storing relatively large amounts of data. Advantageously, the removable storage devices S1 and S2 can be configured to exploit the relative flexibility and the large number of different combinations provided by cascading different subcomponents in different arrangements and structures.

[0169] In an exemplary embodiment, the removable storage devices S1 and S2 can be configured in a distributed manner to store parts of an expression, a license, a contract, a right, a parameter, a condition, a code, data, an e-book file, a music file, and the like. If two or more licenses or contracts are presented, a conflict, if any, can be resolved based on predetermined rules, orders, lists, tables, and the like. For example, one license or contract can be configured to be considered superior to other licenses or contracts, and the information from the superior license or contract can be determined to supercede the information from the inferior licenses or contracts.

[0170] In another exemplary embodiment, an interpreter, such as the interpreter 212, and the like, can be configured to be distributed and stored using different removable storage media, such the removable storage devices S3, S4 and S5. Advantageously, the exemplary embodiments provide a relatively more flexible, cheaper, smaller, faster, and more object-oriented solution. For example, the removable storage device S3 can be configured to interpret expressions for expiration dates in a relatively fast and efficient manner, the removable storage device S4 can be configured to perform interpretation for page numbers for e-books, and the removable storage device S5 can be configured to perform interpretation for e-money, and the like.

[0171] In an exemplary embodiment, the removable storage devices S1 and S2 can be configured so as to be processed based on order and context. For example, in an order-based interpretation, the interpretation of S1S2 can be configured to be different from the interpretation of S2S1.

[0172] In a context-based interpretation, the interpretation of the removable storage device S1 can be configured to be different when the removable storage devices S1 is cascaded with the removable storage devices S3, instead of the removable storage devices S2. Thus, interpretation of the removable storage device S1 in an S1S2 configuration can be configured to be different from interpretation of S1 in an S1S3 configuration. For example, in the former case S1 can be configured to include a Termination Clause in the corresponding contract, but in the latter case S1 can be configured to not include such a clause.

[0173] In an exemplary embodiment, removable storage medium can be cascaded and employ a common interpreter, interpreters can be cascaded and employ a common removable storage medium, removable storage medium and interpreters can be cascaded, and the like. Advantageously, the exemplary cascading embodiments, for example, provide flexibility and a dynamic nature for legality expression storage and interpretation.

[0174] In an exemplary embodiment, the use of legality or rights and expressions and a removable storage media in the context of wills, advantageously, can be provided. Advantageously, Public Key Infrastructure (PKI) technology, biometrics, and the like, can be employed for security purposes. For example, when the author of an e-book prepares the e-book, the author can associate a will in the form of a legality expression with the e-book. In addition, two or more wills can be combined as one will. For example, in a will of person 1, the person 1 can grant the e-book to person 2 and to person 3. In addition, the person 2 and the person 3 also can have wills specified with legality expressions. The wills can be combined as cascading wills or can be combined in a hierarchical structure, for example, based on implicit or explicit assignments, or based on the applicable laws as default situations, and the like.

[0175] In a further exemplary embodiment, servitudes or easements for lands or other objects, which can be assigned or granted, wherein such rights can be propagated or transferred to others, advantageously, can be specified using legality or rights and expressions.

[0176] In an exemplary embodiment, cascaded removable storage devices, such as the removable storage device 202, can be configured to store legality expressions, for example, that allow access to partial parts of a digital work and which, advantageously, can be extremely beneficial in terms of security. For example, rights to access portions of bits from a digital war zone map can be given to 12 individuals from the Pentagon. For security reasons, each person can be given rights to access {fraction (1/12)}th of the digital bits for the map. Each person then can receive respective rights on a respective removable storage device. In order for the whole map to be visible, the 12 persons can present the respective removable storage devices to a map rendering device at the Pentagon. If anyone attempts to view a portion of the map, such as person would not be able to make sense of the data since the data can be encoded in such a way that the digital bits from all 12 devices need be accessible to make sense of the respective portions of the map.

[0177] Advantageously, the exemplary embodiments can be applied to many other different applications, as will be appreciated by those skilled in the relevant art(s). The various applications can potentially employ distinct method of partitioning or different things to partition. In an exemplary embodiment, such partitioning, for example, can include even/odd partitioning. In addition, partitioning can be based on N modes with M bits, bytes, and the like, where N is the size, length, amount, and the like, and M is the number of partitions desired. Further, the partitioning can be based on any suitable formula, can be based on random partitioning, and the like. In a further exemplary embodiment, the bits, bytes, time segments, pixels, content type, colors, frequencies, images, letters, numbers, symbols, and the like, can be partitioned.

[0178] FIG. 11 is a flowchart for illustrating an exemplary process for expression interpretation and validation that can be employed in the systems of FIGS. 1 and 2-10. In FIG. 11, at step 1102, for example, an expression, such as a legality expression, can be obtained for processing. At step 1104, the expression can be interpreted and if the interpretation is successful, as determined at step 1106, the expression can be validated at step 1108. Otherwise, at step 1114, an error message can be returned for indicating a failure in the interpretation step. If the validation is successful, as determined at step 1110, the expression can be enforced at step 1112. Otherwise, at step 1114, an error message can be returned for indicating a failure in the validation step. The steps 1102-1114 can be repeated for further processing of legality expressions.

[0179] FIG. 12 is a flowchart for illustrating an exemplary process for expression authorization and authentication that can be employed in the systems of FIGS. 1 and 2-10. In FIG. 12, at step 1202, for example, an expression, such as a legality expression, can be obtained for processing. At step 1204, the expression can be interpreted and if the interpretation is successful, as determined at step 1206, the expression can be authorized at step 1208. Otherwise, at step 1216, access can be denied based on the failure in the interpretation step. If the authorization is successful, as determined at step 1210, the expression can be authenticated at step 1212. Otherwise, at step 1216, access can be denied based on the failure in the authorization step. If the authentication is successful, as determined at step 1214, access can be granted at step 1218. Otherwise, at step 1216, access can be denied based on the failure in the authentication step. The steps 1202-1218 can be repeated for further processing of legality expressions.

[0180] The devices and subsystems of the exemplary systems described with respect to FIGS. 1-12 can communicate, for example, over a communications network 170 or 870, and can include any suitable servers, workstations, personal computers (PCs), laptop computers, PDAs, Internet appliances, set top boxes, modems, handheld devices, telephones, cellular telephones, wireless devices, other devices, and the like, capable of performing the processes of the disclosed exemplary embodiments. The devices and subsystems, for example, can communicate with each other using any suitable protocol and can be implemented using a general-purpose computer system, and the like. One or more interface mechanisms can be employed, for example, including Internet access, telecommunications in any suitable form, such as voice, modem, and the like, wireless communications media, and the like. Accordingly, communications network 170 or 870 can include, for example, wireless communications networks, cellular communications networks, satellite communications networks, Public Switched Telephone Networks (PSTNs), Packet Data Networks (PDNs), the Internet, intranets, hybrid communications networks, combinations thereof, and the like. In addition, the communications network 170 or 870 can be the same or different networks.

[0181] As noted above, it is to be understood that the exemplary systems, for example, as described with respect to FIGS. 1-12, are for exemplary purposes, as many variations of the specific hardware used to implement the disclosed exemplary embodiments are possible. For example, the functionality of the devices and the subsystems of the exemplary systems can be implemented via one or more programmed computer systems or devices. To implement such variations as well as other variations, a single computer system can be programmed to perform the special purpose functions of one or more of the devices and subsystems of the exemplary systems. On the other hand, two or more programmed computer systems or devices can be substituted for any one of the devices and subsystems of the exemplary systems. Accordingly, principles and advantages of distributed processing, such as redundancy, replication, and the like, also can be implemented, as desired, for example, to increase the robustness and performance of the exemplary systems described with respect to FIGS. 1-12.

[0182] The exemplary systems described with respect to FIGS. 1-12 can be used to store information relating to various processes described herein. This information can be stored in one or more memories, such as a hard disk, optical disk, magneto-optical disk, RAM, and the like, of the devices and sub-

systems of the exemplary systems. One or more databases of the devices and subsystems can store the information used to implement the exemplary embodiments. The databases can be organized using data structures, such as records, tables, arrays, fields, graphs, trees, lists, and the like, included in one or more memories, such as the memories listed above.

[0183] All or a portion of the exemplary systems described with respect to FIGS. 1-12 can be conveniently implemented using one or more general-purpose computer systems, microprocessors, digital signal processors, micro-controllers, and the like, programmed according to the teachings of the disclosed exemplary embodiments. Appropriate software can be readily prepared by programmers of ordinary skill based on the teachings of the disclosed exemplary embodiments. In addition, the exemplary systems can be implemented by the preparation of application-specific integrated circuits or by interconnecting an appropriate network of component circuits.

[0184] Advantageously, the exemplary embodiments described herein can be employed in offline systems, online systems, and the like, and in applications, such as TV applications, computer applications, DVD applications, VCR applications, appliance applications, CD player applications, and the like. In addition, the signals employed to transmit the legality expression of the exemplary embodiments, can be configured to be transmitted within the visible spectrum of a human, within the audible spectrum of a human, not within the visible spectrum of a human, not within the audible spectrum of a human, combinations thereof, and the like.

[0185] Although the exemplary embodiments are described in terms of applications in music, games, movies, coupons, legal arenas, and the like, the exemplary embodiments are applicable to any suitable application, such as digital and non-digital content, devices, software, services, goods, resources, and the like, and can be practiced with variations in technology, interface, language, grammar, content, rights, offerings, services, speed, size, limitations, devices, and the like.

[0186] While the present invention have been described in connection with a number of exemplary embodiments and implementations, the present invention is not so limited but rather covers various modifications and equivalent arrangements, which fall within the purview of the appended claims.

* * * * *

