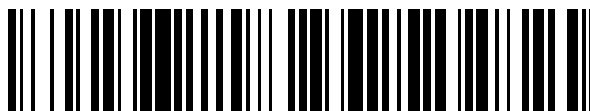


19



OFICINA ESPAÑOLA DE
PATENTES Y MARCAS

ESPAÑA



11 Número de publicación: **2 266 514**

51 Int. Cl.:

G06F 17/00 (2006.01)

G06F 1/00 (2006.01)

12

TRADUCCIÓN DE PATENTE EUROPEA MODIFICADA
TRAS OPOSICIÓN

T5

96 Fecha de presentación y número de la solicitud europea: **06.06.2002 E 02739716 (5)**

97 Fecha y número de publicación de la concesión europea modificada tras oposición: **03.06.2015 EP 1309926**

54

Título: **Método y sistema de gestión de derechos digitales de abono**

30

Prioridad:

07.06.2001 US 296114 P

45

Fecha de publicación y mención en BOPI de la
traducción de la patente modificada:
30.09.2015

73

Titular/es:

**CONTENTGUARD HOLDINGS, INC. (100.0%)
6900 N. Dallas Parkway, Suite 850
Plano TX 75024, US**

72

Inventor/es:

LAO, GUILLERMO

74

Agente/Representante:

UNGRÍA LÓPEZ, Javier

ES 2 266 514 T5

DESCRIPCIÓN

Método y sistema de gestión de derechos digitales de abono

5 La presente invención se refiere a un sistema de gestión de derechos digitales de abono y su método. En particular, la presente invención se refiere a dicho sistema y método que facilita el abono a múltiples elementos protegidos, tal como contenido digital.

10 Una de las cuestiones más importantes que impiden la amplia distribución de obras digitales (es decir, documentos u otro contenido en formas legibles por ordenador), mediante medios electrónicos, e Internet en particular, es la falta corriente de la capacidad de hacer valer los derechos de propiedad intelectual de los propietarios de contenidos durante la distribución y el uso de obras digitales. Los esfuerzos por resolver este problema se han denominado "Gestión de derechos de propiedad intelectual" ("IPRM"), "Gestión de derechos de propiedad digital" ("DPRM"), "Gestión de propiedad intelectual" ("IPM"), "Gestión de derechos" ("RM"), y "Gestión de copyright electrónico" ("ECM"), denominados aquí en conjunto "Gestión de derechos digitales (DRM)". Son numerosas las cuestiones a considerar al llevar a cabo un sistema DRM. Por ejemplo, se deberán resolver los problemas de autenticación, autorización, justificación, pago y compensación financiera, especificación de derechos, verificación de derechos, aplicación de derechos, y protección de documentos. Las Patentes de Estados Unidos 5.530.235, 5.634.012, 5.715.403, 5.638.443, y 5.629.980 describen sistemas DRM que resuelven estos problemas.

20 En el mundo de los documentos impresos y otro contenido físico, una obra creada por un autor se suele ofrecer a un editor, que formatea e imprime numerosas copias de la obra. Las copias son enviadas posteriormente por un distribuidor a librerías u otras tiendas minoristas, en las que las copias son compradas por los usuarios finales. Aunque la baja calidad de la copia y el alto costo de distribución del material impreso han servido de disuasivos de la copia no autorizada de la mayor parte de los documentos impresos, es demasiado fácil copiar, modificar y redistribuir obras digitales no protegidas con alta calidad. Por consiguiente, se necesitan mecanismos para proteger las obras digitales con el fin de retener los derechos del propietario de la obra.

30 Por desgracia, se ha reconocido ampliamente que es difícil evitar, o incluso disuadir, que las personas hagan copias no autorizadas de obras electrónicas dentro de sistemas de comunicaciones e informáticos de propósito general corrientes como ordenadores personales, estaciones de trabajo, y otros dispositivos conectados por redes de comunicaciones, tales como redes de área local (LANs), intranets e Internet. Muchos intentos de proporcionar soluciones basadas en hardware para evitar la copia no autorizada no han tenido éxito. La proliferación de tecnologías de comunicaciones de anchura de banda alta y el desarrollo de lo que actualmente se conoce como la "Infraestructura de Información Nacional" (NII) hará aún más conveniente distribuir electrónicamente grandes documentos, incluyendo archivos vídeo, tal como películas completas, y así eliminará todos los elementos disuasorios restantes de la copia no autorizada y distribución de obras digitales. Por consiguiente, las tecnologías DRM se están convirtiendo en una alta prioridad.

40 Se ha empleado dos esquemas DRM básicos, contenedores seguros y sistemas de confianza. Un "contenedor seguro" (o simplemente un documento encriptado) ofrece una forma de mantener encriptado el contenido del documento hasta que se cumple un conjunto de condiciones de autorización y se cumplen algunos términos del copyright (por ejemplo, pago por uso). Después de verificar las varias condiciones y términos con el proveedor de documentos, el documento es entregado al usuario en forma clara. Productos comerciales como CRYPTOLOPES™ y DIGIBOXES™ pertenecen a esta categoría. Claramente, el método del contenedor seguro proporciona una solución para proteger el documento durante la entrega por canales inseguros, pero no proporciona ningún mecanismo para evitar que los usuarios legítimos obtengan el documento claro y después lo usen y redistribuyan en violación de la propiedad intelectual de los propietarios de los contenidos.

50 En el método del "sistema de confianza", todo el sistema es responsable de evitar el uso no autorizado y la distribución del documento. Construir un sistema de confianza implica por lo general introducir nuevo hardware tal como un procesador seguro, almacenamiento seguro y dispositivos de presentación seguros. Esto también requiere que se certifique que todas las aplicaciones de software que se ejecutan en sistemas de confianza son de confianza. Aunque la construcción de un sistema de confianza a prueba de manipulación es un reto real para las tecnologías existentes, las tendencias actuales del mercado sugieren que los sistemas abiertos y de confianza, tales como PCs y estaciones de trabajo que usan navegadores para acceder a la web, serán los sistemas dominantes utilizados para acceder a obras digitales. En este sentido, los entornos informáticos existentes, tales como PCs y estaciones de trabajo equipados con sistemas operativos populares (por ejemplo, Windows™, Linux™, y UNIX) y aplicaciones de presentación, tal como navegadores, no son sistemas de confianza y no se pueden convertir en sistemas de confianza sin alterar significativamente sus arquitecturas. Naturalmente, la alteración de la arquitectura frustra una finalidad primaria de la web, es decir, la flexibilidad y compatibilidad.

65 La Patente de Estados Unidos 5.634.012 describe un sistema para controlar la distribución de documentos digitales. Cada dispositivo de presentación tiene un depósito asociado. Un conjunto predeterminado de pasos de transacción de uso define un protocolo utilizado por los depósitos para aplicar derechos de uso asociados con un documento. Los derechos de uso persisten con el contenido del documento. Los derechos de uso pueden permitir varias

maneras de uso tales como ver solamente, usar una sola vez, distribución, y análogos. Los derechos de uso pueden depender del pago u otras condiciones.

Los sistemas DRM convencionales proporcionan típicamente acceso al contenido protegido después de una transacción en la que un usuario final obtiene una licencia que permite el acceso al contenido protegido. Así, los sistemas DRM convencionales utilizan un modelo "por transacción", donde cada acceso al contenido protegido requiere una transacción separada con una licencia separada. A este respecto, los sistemas DRM convencionales pueden ser muy incómodos cuando un usuario espera acceder a gran número de elementos de contenido protegido dado que se debe realizar una transacción para cada elemento al que se acceda.

US-A-5 917 912 describe un sistema y métodos para la protección de derechos electrónicos. Una tabla de derechos de usuario en la realización ejemplar proporciona autorización y otra información específica a usuarios particulares o grupos de usuarios y combinaciones de objetos expuestas en una tabla de materias 462. Unos registros de permisos 808 pueden proporcionar un universo de permisos para una combinación particular de objetos-usuarios. Según otra realización, un depósito tiene dos zonas funcionales principales: un sistema de contenido y un sistema de cámara de compensación. El sistema de contenido se compone de un sistema de registro de usuario/autor, un catálogo de contenidos, un mecanismo de búsqueda, almacenamiento de contenidos, referencias de contenidos, y un sistema de envío compuesto por un empaquetador de control, un empaquetador de contenedor, y un sistema de transacciones. Según un ejemplo donde se utilizan "reglas y controles", el "proceso de eventos" 402 detecta cosas que suceden y determina qué "eventos" precisan acción por parte de los otros "procesos". El hecho de que un "evento" necesite más procesamiento depende de las "reglas y controles" correspondientes al contenido. Según otra realización, un usuario final pide contenido del depósito VDE (por ejemplo, mediante selección en un menú de opciones disponibles), el sistema de contenidos 3302A localiza el contenido en las referencias de contenidos y/o en el dispositivo de almacenamiento de contenidos. El sistema de contenidos 3302A puede hacer referencia posteriormente a la información guardada en el catálogo de contenidos 3322, el perfil de cuenta del usuario final, y/o el perfil de cuenta del autor para determinar la naturaleza exacta de formato del contenedor y/o la información de control que puede ser necesaria para crear un contenedor de contenido VDE para satisfacer la petición del usuario final. Según otro aspecto, los servicios ROS proporcionados usando un procesador central 654 y/o un procesador seguro (SPU 500) se enlazan en la realización preferida usando una estructura de petición de procesamiento interno de "llamada de procedimiento remoto".

El documento EP 0 715 244 A1 desvela un sistema para controlar la distribución y uso de trabajos digitales utilizando una gramática de derechos de uso. Una transacción de uso entre dos repositorios que aplican los derechos de uso. La transacción de uso se realiza después de que se establece la confianza entre ambos repositorios. Para establecer la confianza, se usan certificados con claves públicas, que se proporcionan en los repositorios mediante un repositorio maestro.

El objeto de la presente invención es proporcionar un sistema mejorado de gestión de derechos y un método correspondiente para gestionar el uso de elementos que tienen derechos de uso asociados.

Este objeto se logra con la materia objeto de las reivindicaciones independientes 1 y 13.

Realizaciones preferidas se definen por la materia objeto de las reivindicaciones dependientes.

Un primer aspecto de la invención es un sistema DRM para distribuir elementos que tienen derechos de uso asociados según una realización de la presente invención, incluyendo un dispositivo de activación adaptado para facilitar un paquete de software que aplica derechos de uso para controlar el uso de los elementos, teniendo el paquete de software un par de claves pública y privada, estando asociada la clave pública con un usuario, un dispositivo de licencia adaptado para conceder una licencia que tiene derechos de uso asociados con al menos un elemento, un dispositivo de uso adaptado para recibir el paquete de software, recibir la licencia asociada con el al menos único elemento, y permitir al usuario acceder al menos al único elemento según la licencia, y un dispositivo de gestión de abonos adaptado para mantener una lista de abonos incluyendo la clave pública asociada con el usuario, donde la licencia es concedida por el dispositivo de licencia después de verificar la presencia de la clave pública en la lista de abonos.

Un segundo aspecto de la presente invención es un método para distribuir elementos que tienen derechos de uso asociados, incluyendo el método los pasos de proporcionar un paquete de software a al menos un usuario, aplicando el paquete de software derechos de uso para controlar el uso de los elementos y teniendo una clave privada y una clave pública asociadas con el al menos único usuario, almacenar la clave pública asociada con el al menos único usuario en una lista de abonos, recibir una petición del al menos único usuario para acceder al menos al único elemento, verificar que el al menos único usuario que pide acceso a al menos un elemento figura en la lista de abonos, y conceder una licencia que concede derechos de uso a al menos un usuario para usar el al menos único elemento.

La figura 1 es una ilustración esquemática de un sistema DRM adaptado para un modelo por transacción.

La figura 2 es una ilustración esquemática de una etiqueta de derechos de la realización preferida.

La figura 3 es una ilustración esquemática de una licencia de la realización preferida.

- 5 La figura 4 es una ilustración esquemática de un sistema DRM según una realización de la presente invención que proporciona acceso de abono al contenido protegido.

Y la figura 5 es un diagrama de flujo de un método de la realización preferida.

- 10 Se puede utilizar un sistema DRM para especificar y aplicar derechos de uso para elementos, tal como contenido digital, servicios, o propiedad de artículos. La figura 1 ilustra un sistema DRM 10 que se puede usar para distribuir contenido digital. El sistema DRM 10 incluye un componente de activación de usuario, en forma de servidor de activación 20, que concede pares de claves pública y privada a usuarios de contenido de una manera protegida, como es conocido.

- 15 Típicamente, cuando un usuario usa un sistema DRM 10 por vez primera, el usuario es activado. Durante un proceso de activación, se intercambia alguna información entre el servidor de activación 20 y un dispositivo asociado con el usuario, tal como el entorno del cliente 30, y el componente de cliente 60 es descargado e instalado en el entorno de cliente 30. El componente de cliente 60 es preferiblemente resistente a las falsificaciones y contiene el conjunto de claves pública y privada concedidas por el servidor de activación 20 así como otros componentes, tales como algún motor necesario para analizar o presentar elementos protegidos, tales como el contenido protegido 42.

- 20 La etiqueta de derechos 40 está asociada con el contenido protegido 42 y especifica derechos de uso que están disponibles para un usuario final cuando se cumplen condiciones correspondientes. El contenido protegido 42 especifica un elemento específico, como se describe más adelante. El servidor de licencias 50 gestiona las claves de encriptado y concede licencias 52 para el ejercicio de derechos de la manera expuesta más adelante. Las licencias 52 expresan la concesión real de derechos a un usuario final. Por ejemplo, la licencia 52 puede permitir a un usuario ver el contenido protegido 42 por una tarifa de cinco dólares. El componente de cliente 60 interpreta y aplica los derechos que han sido especificados en la licencia 52.

- 30 La figura 2 ilustra una etiqueta de derechos 40 según la realización preferida. La etiqueta de derechos 40 incluye múltiples ofertas de derechos 44. Cada oferta de derechos 44 incluye derechos de uso 44a, condiciones 44b, y especificación de contenido 44c. La especificación de contenido 44c puede incluir cualquier mecanismo para referenciar, llamar, localizar, o especificar de otro modo el contenido 42 asociado con la oferta de derechos 44.

- 35 La figura 3 ilustra una licencia 52 según la realización preferida. La licencia 52 incluye una ID de licencia única 52a, otorgamiento 52b (incluyendo derechos de uso, principal, condiciones, y variables de estado) y una especificación de contenido que designa el contenido 42 asociado con la licencia 52. La licencia 52 también incluye la firma digital 52c incluyendo claves criptográficas o análogos para desbloquear un ticket de elemento 42.

- 40 Los derechos de uso especifican formas de uso. Por ejemplo, una forma de uso puede incluir la capacidad de usar un elemento en una forma especificada tal como imprimir, copiar, ver, o análogos. Los derechos también pueden estar agrupados. Además, los derechos de uso pueden especificar derechos de transferencia, tal como derechos de distribución. En algunos casos hay que cumplir condiciones con el fin de ejercer la forma de usar un derecho de uso especificado. Por ejemplo, una condición puede ser el pago de una tarifa, la presentación de datos personales, o cualquier otro requisito deseado antes de permitir el ejercicio de una forma de uso. Las condiciones también pueden ser "condiciones de acceso", por ejemplo, se puede aplicar condiciones de acceso a un grupo particular de usuarios, por ejemplo estudiantes en una universidad, o miembros de un club de lectores. En otros términos, la condición es que el usuario sea una persona particular o miembro de un grupo particular. Los derechos y las condiciones pueden existir como entidades separadas o se pueden combinar. Las variables de estado realizan el seguimiento de las condiciones de estado potencialmente dinámicas. Las variables de estado son variables que tienen valores que representan el estado de un elemento, derechos de uso, licencia u otras condiciones dinámicas. Las variables de estado pueden ser rastreadas, por la cámara de compensación 90 u otro dispositivo, en base a mecanismos de identificación en la licencia 52 y ticket 42. Además, el valor de las variables de estado se puede usar en una condición. Por ejemplo, un derecho de uso puede ser el derecho a redimir el ticket de elemento 42 para bienes especificados, y una condición puede ser que el derecho de uso se pueda ejercer tres veces. Cada vez que se ejerce el derecho de uso, se incrementa el valor de la variable de estado. En este ejemplo, cuando el valor de la variable de estado es tres, la condición ya no se cumple y el ticket 42 no puede ser redimido. Otro ejemplo de una variable de estado es el tiempo. Una condición de la licencia 52 puede requerir que el ticket de elemento 42 se redima dentro de treinta días. Se puede usar una variable de estado para realizar el seguimiento del vencimiento de treinta días. Además, el estado de un derecho de uso puede ser rastreado como una colección de variables de estado. La colección de cambios es el estado de un derecho de uso que representa la historia de uso de ese derecho.

- 65 El contenido protegido 42 se puede preparar con la aplicación de preparación de documentos 72 instalada en un ordenador 70 asociado con el distribuidor de contenido, un proveedor de servicios de contenido, o cualquier otra

parte. La preparación del contenido protegido 42 consiste en especificar los derechos y las condiciones bajo las que el contenido protegido 42 se puede usar asociando una etiqueta de derechos 40 con el contenido protegido 42 y protegiendo el contenido protegido 42 con algún criptoalgoritmo u otro mecanismo para evitar el procesado o la presentación del contenido protegido 42. Se puede usar un lenguaje de derechos, tal como XrML™, para especificar los derechos y las condiciones en la etiqueta de derechos 40. Sin embargo, los derechos y las condiciones se pueden especificar de cualquier manera. Por consiguiente, el proceso de especificar derechos se refiere a cualquier proceso para asociar derechos con el contenido protegido 42. La etiqueta de derechos 40 asociada con el contenido protegido 42 y la clave de encriptado usada para encriptar el contenido protegido 42 se pueden transmitir al servidor de licencias 50. El contenido protegido 42 puede ser un archivo de texto, un archivo audio, un archivo vídeo, un archivo multimedia digital, o cualquier otro contenido digital.

Un flujo de trabajo típico para sistema DRM 10 se describe más adelante. Un usuario que opera dentro del entorno de cliente 30 es activado para recibir el contenido protegido 42 por el servidor de activación 20. Esto da lugar a que un par de claves pública-privada (y posiblemente alguna información específica de usuario/máquina) sea descargada al entorno del cliente 30 en la forma de componente de software de cliente 60 de manera conocida. Este proceso de activación se puede llevar a cabo en cualquier momento antes de la concesión de una licencia.

Cuando un usuario desea obtener un contenido protegido específico 42, el usuario hace una petición referente al contenido protegido 42. Por ejemplo, un usuario podría navegar por un sitio web que se ejecuta en el servidor web del vendedor 80, utilizando un navegador instalado en el entorno de cliente 30, y pedir un elemento correspondiente al contenido protegido 42. El usuario puede examinar ofertas de derechos 44 en la etiqueta de derechos 40 asociada con el contenido protegido 42 y seleccionar los derechos de uso deseados. Durante este proceso, el usuario puede realizar una serie de pasos para cumplir posiblemente las condiciones de los derechos de uso incluyendo una transacción de tarifa u otras transacciones (tal como recogida de información). Cuando se cumplen las condiciones apropiadas y otros prerrequisitos, tal como el cobro de una tarifa y la verificación de que el usuario ha sido activado, el vendedor 80 contacta con el servidor de licencias 50 a través de un canal de comunicaciones seguro, tal como un canal que usa una Secure Sockets Layer (SSL). El servidor de licencias 50 genera entonces una licencia 52 para el contenido protegido 42 y el vendedor 80 hace que se descarguen el contenido protegido 42 y la licencia 52. La licencia 52 incluye los derechos de uso seleccionados y se puede descargar del servidor de licencias 50 o un dispositivo asociado. El contenido protegido 42 se puede descargar del ordenador 70 asociado con un vendedor, distribuidor, u otra parte.

El componente de cliente 60 en el entorno de cliente 30 procederá entonces a interpretar la licencia 52 y permitir el uso del contenido protegido 42 en base a los derechos y condiciones especificadas en la licencia 52. La interpretación y la aplicación de derechos de uso y sistemas y técnicas relacionados son conocidas. Los pasos anteriores pueden tener lugar secuencialmente o de forma aproximadamente simultánea o en varios órdenes secuenciales.

El sistema DRM 10 resuelve aspectos de seguridad de los contenidos protegidos 42. En particular, el sistema DRM 10 puede autenticar una licencia 52 que ha sido concedida por el servidor de licencias 50. Una forma de llevar a cabo tal autenticación es que la aplicación 60 determine si las licencias 52 pueden ser de confianza. En otros términos, la aplicación 60 tiene la capacidad de verificar y validar la firma criptográfica, u otra característica identificativa de la licencia 52. Naturalmente, el ejemplo anterior es simplemente una forma de llevar a la práctica un sistema DRM. Por ejemplo, la licencia 52 y el contenido protegido 42 se pueden distribuir desde diferentes entidades. La cámara de compensación 90 se puede usar para procesar transacciones de pago y verificar el pago antes de conceder una licencia.

Los sistemas DRM, tal como el descrito anteriormente, proporcionan acceso a elementos protegidos, tales como el contenido protegido, después de la activación en la que un usuario final obtiene software y una licencia para acceder al contenido protegido. Se concede una licencia, y así se debe cumplir un intercambio de claves u otros mecanismos de identificación, para cada elemento de contenido protegido. Este modelo por transacción puede resultar incómodo cuando un usuario espera acceder y usar gran número de elementos de contenido protegido, dado que se debe generar una licencia para cada contenido protegido. En contraposición, el sistema DRM y el método según la realización preferida se implementan usando un modo de abono para proporcionar acceso automático de usuario a una colección de contenidos protegidos sin necesitar la activación de una licencia por cada contenido protegido al que se acceda.

Se deberá observar inicialmente que el término "abono" se utiliza en un sentido genérico e incluye cualquier elemento, como el contenido protegido, al que se le permite el acceso a un usuario. El abono podría implicar la entrega de un documento electrónico, o la entrega de unos medios para obtener un documento en papel u otros bienes o servicios. Por ejemplo, los abonos pueden ser publicaciones periódicas, facturas mensuales o extractos de cuentas bancarias o acceso a un servicio continuo de medios. El abono también pueden ser abonos a tickets u otros vales que se utilizan para acceder u obtener otro contenido, recursos, bienes físicos o servicio.

Además, se deberá entender que mientras que los términos "servidor" y "cliente" se utilizan más adelante para describir los dispositivos para implementar la presente invención en la realización aquí explicada, estos términos se

deberán entender en sentido amplio significando cualquier dispositivo apropiado para ejecutar la función descrita. Por ejemplo, se puede usar un ordenador personal, ordenador portátil, PDA u otro dispositivo de mano, PDAs, o cualquier otro ordenador programable de propósito general, o combinación de tales dispositivos, tal como una red de ordenadores.

5 El sistema DRM 100 según una realización de la presente invención se ilustra en la figura 4. El sistema DRM 100 permite el uso, basado en abono, de elementos, tales como el contenido protegido 108. Dado que los elementos de contenido protegido 108 están encriptados o protegidos de otro modo, no pueden ser usados por usuarios finales 114 sin licencias 116 y un paquete de software 103 como un componente de seguridad. El sistema DRM 100 incluye
10 un dispositivo de activación como un servidor de activación 102 que está adaptado para entregar un paquete de software 103 a un dispositivo de uso, tal como un cliente 106, para permitir que uno o varios usuarios finales 114 usen una pluralidad de elementos de contenido protegido 108. El servidor de activación 102 del sistema DRM 100 proporciona un par de claves pública y privada al cliente 106, teniendo cada uno de los usuarios finales 114 al menos una clave pública asociada.

15 El sistema DRM 100 también incluye un dispositivo de licencia, tal como un servidor de licencias 110, que está adaptado para conceder licencias 116 que tienen derechos de uso asociados con una pluralidad de contenidos protegidos 108. Estas licencias 116 definen los derechos del usuario final relativos a un elemento particular del contenido protegido 108. Las peticiones de licencias 116 al servidor de licencias 110 las realiza el punto de
20 distribución 128 en base a peticiones de usuarios finales 114 mediante el cliente 106. Un dispositivo de cliente separado puede estar asociado con cada usuario final 114, o los usuarios finales 114 pueden usar un dispositivo de cliente común. La licencia 116 permite a los usuarios finales autorizados 114 acceder y usar el contenido protegido 103. Cuando el servidor de licencias 110 concede licencias solicitadas 116', el punto de distribución 128 pre-empaqueta las licencias 116' con el contenido protegido apropiado 108 de manera que las licencias 116' estén
25 adaptadas al contenido protegido 108 como se representa en la figura 4. Cuando están pre-empaquetadas, las licencias 116' puede ser una parte de contenido protegido 108 de la manera representada en la figura 4. Sin embargo, las licencias 116' también pueden ser un archivo separado u otro componente con un mecanismo para asociar la licencia al contenido protegido apropiado. Por ejemplo, se puede usar un enlace, una referencia, una llamada u otro mecanismo de asociación. El cliente 106 recibe un paquete de software 103 del servidor de activación
30 102, recibe el contenido protegido 108 con la licencia 116' asociada en una forma pre-empaquetada del punto de distribución 128, y permite que uno o más usuarios finales 114 accedan al contenido protegido 108 para el que el usuario final está autorizado.

35 En la implementación basada en abono, el sistema DRM 100 permite a los usuarios finales 114 acceder a una pluralidad de contenidos protegidos 108 sin necesitar una activación separada para cada elemento de contenido protegido. En particular, el sistema DRM 100 está adaptado para operar a base de abono y para proporcionar a los usuarios finales abonados 114 el acceso a una pluralidad de elementos de contenido protegido 108 sin requerir activaciones adicionales por parte del servidor de activación 102 y el retardo y recursos correspondientes.

40 El sistema DRM 100 de la presente realización está provisto de un dispositivo de gestión a abonos, tal como un gestor de lista de abonos 120, que está adaptado para reconocer la identidad de cada usuario final 114 manteniendo una lista de abonos de claves públicas asociadas con cada usuario final abonado 114. El gestor de lista de abonos 120 de la realización ilustrada también está provisto de una base de datos 122 para almacenar dicha información de identidad e información de clave pública asociada con los usuarios finales 114. Teniendo una lista de abonos y
45 comparando la clave pública utilizada con las claves públicas en la lista de abonos, el sistema DRM 100 conoce la identidad de los usuarios finales abonados 114 que desean acceder y usar el contenido protegido específico. Cuando el punto de distribución 128 pide una licencia en nombre de un usuario final particular que es un abonado, la clave pública asociada con el usuario final particular es extraída de la lista almacenada en la base de datos 122 por el gestor de lista de abonos 120, y la clave pública es utilizada por el servidor de licencias 110 para conceder la
50 licencia necesaria.

En la realización ilustrada de la figura 4, el sistema DRM 100 se usaría de la siguiente manera para realizar el método ilustrado en la figura 5. Primero, los usuarios finales 114 utilizan el entorno de cliente 106 a activar por el servidor 102 de la manera descrita anteriormente (paso 502). Los usuarios finales 114 se adhieren a un abono que
55 se ofrece a través de un punto de distribución 128 que se puede implementar como una aplicación a través de un sitio web, un dispositivo de almacenamiento en línea, o de otra manera apropiada en el paso 504. Durante el proceso de adhesión a un abono, se puede prever una serie de pasos para crear una cuenta o realizar el pago de una tarifa de cualquier manera apropiada. Los detalles de la creación de la cuenta o el pago de la tarifa se pueden llevar a cabo usando interfaces de usuario conocidas y APIs conocidas, o análogos y por ello no se explican aquí
60 con mayor detalle.

Después de recibir una petición de contenido en el paso 506, el punto de distribución 128 recupera las claves públicas que están asociadas con cada usuario final 114, pidiendo el contenido protegido 108, las claves públicas obtenidas durante el proceso de activación de servidor de activación 102. Las claves públicas identifican a usuarios
65 finales y se guardan en una base de datos 122 en correspondencia con el usuario final asociado y otros datos asociados. Cuando el contenido protegido 108 se ha de distribuir a usuarios finales abonados 114, por ejemplo a

través de correo electrónico, el punto de distribución 128 realiza peticiones al servidor de licencias 110 para que conceda las licencias apropiadas. Las peticiones de licencias pueden incluir una lista de usuarios finales, sus claves de encriptado públicas respectivas, y la ID del contenido protegido para el que se han de conceder las licencias. Naturalmente, la petición también podría ser para licenciar un usuario final único o también para contenido protegido múltiple. La petición de licencias se puede ejecutar usando una API o por cualquier otro protocolo apropiado.

El servidor de licencias 110 autentica posteriormente al solicitante, tal como un punto de distribución 128, comprueba que los usuarios finales están en la lista apropiada de abonos (paso 508), y si es así, concede licencias 116 (paso 510), y las entrega al punto de distribución 128 para pre-empaquetado con el contenido protegido 108. El punto de distribución 128 preempaqueta el contenido protegido 108 con las licencias 116' y las entrega, o las pone de otro modo a disposición, a cada usuario final 114 (paso 512). Dado que elementos de contenido protegido 108 se entregan preempaquetados con una licencia concedida 116, los usuarios no tendrían que realizar activaciones/procedimientos adicionales y esperar que se concedan licencias para acceder y usar el contenido protegido 108 del abono después de la activación inicial. Las listas de abonos son mantenidas por el gestor de lista de abonos 120 y correlacionadas con las claves públicas, para verificar si el usuario tiene derecho a una licencia 116.

Como se ha indicado anteriormente, es deseable preempaquetar una licencia 116' con contenido 108 cuando es entregada por el punto de distribución 128 a usuarios finales 114 con el fin de proporcionar una experiencia de usuario más continua. En la realización ilustrada de la figura 4, el punto de distribución 128, que se representa solamente de forma esquemática, puede ser una aplicación informática o un escaparate tal como una tienda basado en web o vendedor en línea. Alternativamente, el punto de distribución 128 puede ser una aplicación informática que se integra con un servidor de correo, el servidor de licencias 110, o el gestor de lista de abonos 120 que mantiene una lista de abonos. En tales realizaciones, el mantenimiento de la lista de abonos podría ser tan simple como almacenar las claves públicas en una base de datos 122, dentro de un directorio de servidor de correo, o un enlace a otra posición de almacenamiento donde las claves públicas se pueden almacenar y gestionar. En una empresa tal como un grupo, compañía o entidad, las listas de distribución pueden estar adaptadas a las listas de abonos. Se puede gestionar cualquier número de listas de abonos.

De la manera antes descrita, el sistema DRM 100 facilita a los usuarios finales acceso a gran número de elementos de contenido protegido sin necesidad de activaciones repetidas por cada licencia. También se deberá observar que la secuencia de pasos antes explicada ilustra solamente un flujo ejemplar de cómo puede operar un sistema DRM según la presente invención, uno o varios pasos pueden tener lugar en un orden diferente, o de forma aproximadamente simultánea.

En una realización donde el punto de distribución 128 es una aplicación dentro de un servidor de correo, el punto de distribución 128 puede operar para interceptar el contenido protegido entrante con el fin de proteger su acceso, y pedir al servidor de licencias 110 una licencia para uno o más usuarios finales 114 que están abonados. El punto de distribución 128 puede preempaquetar entonces el contenido protegido y proporcionar el contenido preempaquetado al flujo del servidor de correo de manera que el servidor de correo pueda dirigir el contenido protegido a los usuarios finales.

En una realización donde el punto de distribución 128 se integra con el gestor de lista de abonados 120, las claves públicas asociadas con usuarios finales 114 y mantenidas como una lista de identidades de usuarios finales son típicamente, pero no necesariamente, descargadas del cliente 106 durante el proceso de activación con el servidor de activación 102. Además, en una empresa, el gestor de lista de abonos 120 puede estar integrado con un sistema de servicios de directorio o sistema similar. La lista de usuario finales también puede incluir una lista de contenidos a la que se abona cada uno de los usuarios finales, además de la información de identidad y las claves públicas.

Además, el acceso al contenido protegido puede ser a través de un modelo de descarga donde los usuarios finales buscan de forma pro-activa y usan el contenido protegido, por ejemplo descargando el contenido protegido de un sitio web. Alternativamente, el acceso al contenido protegido puede ser a través de un modelo de envío donde los usuarios finales reciben el contenido protegido a través de correo electrónico, anexo a correo electrónico, o por otro mecanismo.

Una ventaja significativa de sistema DRM 100 es que permite la automatización del acceso del usuario final a una colección de contenidos protegidos cuando el usuario final es un miembro de un grupo de abonados designado para un abono particular. Varios usuarios finales pueden abonarse y borrarse y la lista de abonos puede ser gestionada por los usuarios finales, o gestionada por otra persona o sistema de gestión automático. La automatización del acceso del usuario final también permite que el proceso para obtener una licencia para acceder al contenido protegido particular sea transparente al usuario final. Por ejemplo, en el modelo de descarga, un usuario final puede realizar descarga o acceder de otro modo a una pluralidad de contenidos protegidos sin pasos de transacción adicionales para obtener el software o las licencias requeridas para cada contenido protegido al que se acceda después de la activación inicial. En el modelo de envío, el usuario final recibe el contenido protegido a través de correo electrónico, anexo a correo electrónico, o por otro mecanismo que se puede abrir sin pasos de transacción adicionales después de la activación inicial.

Se deberá notar que la entrega actual de la licencia y/o el contenido protegido se pueden realizar de varias formas, por ejemplo, por sistemas especializados tales como motores de entrega. Los motores de entrega son entidades especializadas y altamente eficientes que entregan contenido a una población grande. Por ejemplo, una compañía de corretaje puede usar motores de entrega para entregar confirmaciones de transacciones en bolsa contratando esta tarea con una compañía especializada en entrega a bajo costo de tales documentos.

Ejemplos de tipos específicos de abonos previstos para uso con la realización preferida son abonos de “abonar y alquilar”, y abonos de “abonar y adquirir”. En los abonos de abonar y alquilar, un usuario final sólo puede acceder al contenido protegido siendo al mismo tiempo un abonado activo, o en base a alguna otra condición, por ejemplo, un período de tiempo, un número de vistas, o hasta que esté disponible la versión siguiente del contenido. Un ejemplo de un tipo de abono de abonar y alquilar es el uso en línea de medios continuos. Típicamente, contenido protegido se usaría en línea y una vez que caduca el abono o transcurre un período de tiempo, el contenido protegido, incluyendo el contenido previamente accesible, así como el contenido no accedido, ya no está disponible para el usuario final. En este tipo de abono, los derechos de uso, las condiciones, y las variables de estado se pueden usar para limitar la manera de usar de manera conocida.

En los abonos de abonar y adquirir, los usuarios finales adquieren realmente el contenido protegido. Por ejemplo, una cierta cantidad o tipo de contenido protegido podría adquirirse de una colección más grande incluyendo una pluralidad de contenidos protegidos. Además, podría haber precios preferentes, acceso, o términos especiales para un usuario final abonado. En los abonos de abonar y adquirir, una vez que el contenido protegido es adquirido legítimamente, un usuario final tendría el derecho de usarlo indefinidamente y vencimiento del abono no pone fin en general al derecho a usar el contenido previamente adquirido. Los documentos comerciales, tales como confirmaciones de transacciones en bolsa, son un ejemplo típico de un documento protegido apropiado para el abono de abonar y adquirir.

Naturalmente, en otras implementaciones se pueden combinar ambos tipos de abono. Por ejemplo, a un usuario final abonado se le puede ofrecer un paquete que incluya acceso en línea a todo el contenido protegido y un número predeterminado de descargas. En una aplicación de música, un usuario final abonado puede tener acceso en línea al catálogo completo de títulos musicales, pero sólo está autorizado a descargar cien títulos. Naturalmente, otras permutaciones y modelos de abono son posibles al implementar un sistema y método DRM basado en abono. Por ejemplo, en otro ejemplo, un sistema y método DRM basado en abono concedería derechos a un número específico, por ejemplo cien, descargas a posponer, acumular, o transferir a otra persona, o incluso devolver al proveedor de abonos. Además, por ejemplo, se podría hacer que la adquisición durase solamente lo que duren algunas condiciones y no tiene que ser literalmente para un período indefinido.

Además, se puede aplicar diferentes modelos de abono a diferentes partes del contenido protegido. Por ejemplo, una publicación periódica se pueden adquirir en base de abono y adquisición, pero las imágenes que son parte de la publicación periódica se pueden adquirir en base de abono y alquiler y así podrían expirar o requerir tarifas adicionales, por ejemplo. La licencia asociada con el contenido protegido particular definiría el diferente tratamiento entre la publicación periódica propiamente dicha y sus imágenes. Una vez descargado, el contenido protegido puede ser accedido y usado por el usuario final fuera de línea de la manera determinada por la licencia asociada con el contenido protegido. Con una combinación de abono en línea y fuera de línea, se pueden construir muchos modelos usando el sistema y método DRM basado en abono de la presente invención.

Como un ejemplo, se puede usar un sistema DRM basado en abono en una aplicación de escaparate. Un escaparate puede ser cualquier sitio de comercio electrónico en línea que ofrezca a la venta contenido protegido. A este respecto, el punto de distribución 128 representado en el sistema DRM 100 de la figura 2 puede ser tal escaparate. El usuario final 114 activa el cliente 106 y obtiene claves pública y privada. El usuario final se adhiere entonces a una lista de abonos respondiendo a una oferta de abono en el escaparate y realiza el pago, o cumple otras condiciones. El gestor de lista de abonos 120 toma cada clave pública y asocia la clave pública con la identidad de usuario final. El usuario final intenta entonces descargar el contenido protegido tal como un documento que es parte de una colección de abonos. El escaparate valida la pertenencia del usuario final al abono a través del gestor de lista de abonos 120, recupera la clave pública de usuario final del gestor de lista de abonos 120, y pide al servidor de licencias 110 las licencias asociadas con el contenido protegido solicitado. El servidor de licencias 110, después de verificar la autenticidad de la petición, concede licencias 116 al escaparate. El escaparate preempaqueta entonces la licencia con contenido protegido 108 y la pone a disposición para descarga por el usuario final 114, como se ha explicado previamente. El usuario final 114 puede descargar entonces el contenido protegido 108 y usar de forma transparente el contenido protegido 108 de la manera indicada por la licencia concedida.

En otro ejemplo, un sistema y método DRM basado en abono de la presente invención se puede usar en una aplicación de motor de entrega que realiza la entrega segura del contenido protegido, tal como documentos. Por ejemplo, los usuarios finales 114 pueden adherirse como abonado al contenido 108 proporcionado por la compañía A que es propietaria o controla el contenido 108, y activa un cliente mediante el servidor de activación 102 para obtener claves. La compañía A trabaja con la compañía B que ofrece un servicio de entrega digital seguro para contratar la porción de entrega de documentos de su oferta de servicios de abono. La entrega de documentos

contratada puede ser para entrega de informes financieros u otro tipo de documentación que requiera protección y uso restringido. Tal contratación puede ser beneficiosa para la compañía A porque la compañía B puede ser más eficiente y de costo razonable en esta función particular de entrega de documentos. La compañía B sirve así como un gestor de lista de abonos de control de "motor de entrega" 102 para gestionar la lista de usuarios finales 114 que reciben documentos, es decir, una lista de abonos que asocia clientes abonados de la compañía A con su clave pública obtenida durante la etapa de activación. Naturalmente, podría haber más de una lista de abonos, por ejemplo una lista de clientes preferidos, una lista de tipos específicos de clientes, y análogos.

Cuando la compañía A tiene un documento para entregar a sus abonados, prepara el documento y lo suministra a la compañía B para entrega. La compañía A ordena entonces a la compañía B que entregue los documentos a los usuarios en una o varias listas de abonos, por ejemplo, a clientes más preferentes. La compañía B envía una petición al servidor de licencias 110 para conceder licencias 116 para cada cliente, es decir, el usuario 114 en la lista de clientes más preferidos, estando asociado cada cliente con una clave pública particular. Una vez que las licencias solicitadas 116 son concedidas por el servidor de licencias 110, la compañía B recibe licencias 116, pre-empaqueta los documentos con las licencias 116', y las entrega a los clientes abonados en la lista de clientes más preferentes. Dado que los documentos están preempaquetados 116' con la licencia necesaria, los clientes abonados no tienen que realizar una transacción adicional para usar el contenido protegido según la licencia 116. Así, cada usuario final que recibe la licencia preempaquetada puede recibir y acceder al documento protegido de forma transparente sin activaciones adicionales.

Otro ejemplo del sistema y método DRM basado en abono es en una aplicación de empresa. El punto de distribución 128 en tal aplicación puede ser una aplicación informática que se integra con un servidor de correo, u otra aplicación de la empresa. Además, la aplicación de empresa puede mantener la lista de abonos de cualquier manera apropiada previamente descrita. En este ejemplo de aplicación de empresa, los usuarios finales 118, tal como una persona A, una persona B, y una persona C, son activados a través del servidor de activación 122. Cuando la persona A envía un documento protegido a la persona B y la persona C, el punto de distribución 128 intercepta el documento y pide al servidor de licencias 110 una licencia 116 en nombre de la persona B y la persona C. El punto de distribución 128 recupera entonces las claves públicas para la persona B y la persona C y envía las claves públicas al servidor de licencias 110 que concede licencias 116 concediendo a la persona B y a la persona C derechos al documento protegido enviado por la persona A.

Una vez que las licencias 116 son recibidas del servidor de licencias 110, el punto de distribución 128 pre-empaqueta el documento protegido con la licencia concedida 116' y lo inserta en el flujo normal del servidor de correo de manera que el servidor de correo dirija el documento protegido a la persona C y la persona B. La persona B y la persona C pueden acceder entonces y usar el documento recibido de forma transparente cuando comprueban sus correos electrónicos respectivos según la licencia concedida.

Otro ejemplo de sistema y método DRM basado en abono es una aplicación de tienda de música digital. En tal aplicación, una compañía musical, por ejemplo, una tienda de música en línea, puede ofrecer un abono a clientes como los usuarios 114 donde, por una tarifa predeterminada, los usuarios 114 pueden acceder a uso ilimitado (o limitado) en línea de los títulos del catálogo musical de la tienda de música, y descargar un número predeterminado de títulos musicales.

Cuando un usuario abonado 114 desea acceder al catálogo musical de la tienda de música, el sistema DRM autentica el usuario abonado 114 con el servidor de activación 102 y asegura que el usuario se identifique en una lista de abonos de gestor de lista de abonos 120 antes de permitir el acceso al catálogo musical y los títulos que contiene. Como el usuario descarga varios títulos musicales como contenido 108, de la tienda de música, el servidor de licencias 110 puede realizar el seguimiento del número de títulos que el usuario 114 ha descargado de manera que si el número máximo de descargas no ha sido superado, la tienda de música envía una petición al servidor de licencias para generar licencias 116 para los títulos seleccionados. Una vez que el servidor de licencias 110 concede las licencias necesarias, la tienda de música en línea preempaqueta el título protegido con la licencia apropiada 116 utilizando una aplicación de empaquetado de documentos. El usuario puede descargar entonces de forma transparente los títulos seleccionados de la tienda de música.

Además, la licencia a base de abono de la realización preferida permite la activación antes de la existencia del contenido. Por ejemplo, un usuario puede abonarse a recibir un evento continuo en vivo antes del evento.

Se deberá entender de nuevo que mientras que los términos "servidor" y "cliente" se usan para describir los dispositivos para implementar la presente invención en las realizaciones ilustradas anteriores, estos términos se deberán entender en sentido amplio significando cualquier dispositivo o dispositivos apropiados para ejecutar la función descrita.

La comunicación entre los varios dispositivos se puede llevar a cabo a través de cualquier canal, tal como una red de área local (LAN), Internet, puertos de comunicaciones serie, y análogos. Los canales de comunicaciones pueden utilizar tecnología inalámbrica, tal como radiofrecuencia o tecnología de infrarrojos. Los varios elementos de la realización preferida, tal como los varios servidores y bases de datos conectadas a ellos, se segregan por función a

efectos de claridad. Sin embargo, los varios elementos se pueden combinar en un dispositivo o segregarse de manera diferente. Por ejemplo, el paquete de software, y el par de claves pública y privada pueden ser un único archivo ejecutable y archivos de datos, o múltiples archivos o módulos almacenados en el mismo dispositivo o en diferentes dispositivos. El paquete de software puede ser cualquier intercambio de información que permita la activación de licencias y no tiene que incluir una aplicación de presentación, una clave pública puede ser cualquier tipo de distintivo de identificación o código. Además, la función de los varios dispositivos se puede combinar. Por ejemplo, un único dispositivo puede realizar la función de servidor de licencias 110, servidor de activación 102, gestor de lista de abonos 120, y cliente 106. Además, las funciones se pueden combinar o segregar en cualquier número y configuración de dispositivos. Los varios componentes y módulos tienen utilidad separada y pueden existir solos o en combinación.

Se puede usar cualesquiera protocolos, tipos de datos, o estructuras de datos según la invención. Además, cualesquiera medios apropiados de expresar derechos de uso y condiciones se pueden usar al implementar la presente invención. Por ejemplo, como se ha indicado previamente, se puede usar un lenguaje de derechos, por ejemplo una gramática tal como XrMLTM.

Aunque se han mostrado y descrito varias realizaciones según la presente invención, se entiende que la invención no se limita a ellas. La presente invención puede ser cambiada, modificada y aplicada por los expertos en la técnica. Por lo tanto, esta invención no se limita al detalle representado y antes descrito, sino que también incluye todos los cambios y modificaciones que queden abarcados por las reivindicaciones anexas y equivalentes legales.

REIVINDICACIONES

1. Un sistema de gestión de derechos (10; 100) para gestionar el uso de elementos que llevan asociados derechos de uso, siendo dichos elementos elementos protegidos e incluyendo dicho sistema: un dispositivo de activación (20; 102) adaptado para conceder un paquete de software (103) que aplica derechos de uso para controlar el uso de dichos elementos; incluyendo dicho paquete de software (103) un par de claves pública-privada asociado con un usuario abonado (114); un dispositivo de usuario (30; 106) adaptado para recibir dicho paquete de software (103), recibir una licencia (52; 116) que tiene derechos de uso que especifican una manera de uso y está asociada con al menos un elemento, y permitir a dicho usuario abonado (114) acceder a dicho al menos único elemento según dicha licencia (52; 116); medios para recibir una petición de licencia con respecto a un elemento pedido en nombre de al menos un usuario abonado (114); y un dispositivo de licencia (50; 110) adaptado para conceder dicha licencia (52; 116) asociada con dicho al menos único elemento, donde dicho paquete de software (103) se concede a dicho dispositivo de usuario (30; 106) para permitir a dicho usuario abonado (114) usar dicho elemento, estando asociado dicho usuario abonado (114) con dicho dispositivo de usuario (30; 106), y estando encriptado o protegido de manera que dicha licencia y dicho paquete de software se requieren como un componente de seguridad para usar dicho elemento; dicho dispositivo de activación (20; 102) está adaptado además para proporcionar dicho dispositivo de usuario (30; 106) con un componente de cliente (60) que contiene un motor para examinar o presentar elementos protegidos, dicho componente de cliente se instala en el dispositivo de cliente (30; 106) después de la recepción en el dispositivo de usuario (30; 106); siendo dicho componente de cliente (60) para interpretar dichas licencias (52); y proporcionando dicho sistema (10; 100) a los usuarios abonados (114) acceso a una pluralidad de dicho al menos único elemento controlado por dicho paquete de software, incluyendo además dicho sistema: un dispositivo gestor de abonos (120) incluyendo una lista de abonos que tiene claves públicas asociadas con usuarios abonados; y un punto de distribución (128) que pide y recibe la licencia (52; 116) del dispositivo de licencia (50; 110); preempaquetando además dicho punto de distribución la licencia recibida (52; 116) con dicho al menos único elemento; donde dicho dispositivo de licencia (50; 110) concede una licencia (52; 116) en base a la identidad del usuario abonado (114) comunicando con dicho dispositivo gestor de abonos (120) y verificando que la clave pública asociada con dicho al menos único usuario que desea acceder y usar un elemento está en dicha lista de abonos antes de conceder dicha licencia (52; 116); y dicha licencia preempaquetada (116') y al menos un elemento se entregan o ponen a disposición por dicho punto de distribución (128) a dicho dispositivo de usuario (30; 106) asociado con dicho usuario abonado (114); y donde dicha petición de licencia de dicho punto de distribución (128) incluye una lista de usuarios y sus claves públicas respectivas y una ID de contenido para la que se han de conceder las licencias, y donde dicho dispositivo de licencia (50; 110) está adaptado para conceder una licencia (52; 116) para cada uno de dichos usuarios incluido en dicha petición de licencia de dicho punto de distribución.
2. El sistema de gestión de derechos (10; 100) de la reivindicación 1, donde dichas peticiones de licencia de dicho punto de distribución (128) son para contenido protegido múltiple para el que se han de conceder las licencias.
3. El sistema de gestión de derechos (10; 100) de la reivindicación 1, donde dicho al menos único usuario es una pluralidad de usuarios, teniendo cada uno de dichos usuarios una clave pública como un mecanismo de identificación.
4. El sistema de gestión de derechos (10; 100) de la reivindicación 3, donde dicho dispositivo gestor de abonos (120) mantiene una lista de la identidad de usuarios abonados mediante dicha clave pública asociada con cada uno de dichos usuarios.
5. El sistema de gestión de derechos (10; 100) de la reivindicación 4, donde dicho al menos único elemento es una pluralidad de elementos de contenido protegido.
6. El sistema de gestión de derechos (10; 100) de la reivindicación 5, donde dicha pluralidad de elementos de contenido protegido incluye al menos uno de un archivo de texto, un archivo audio, un archivo vídeo, y archivos multimedia digitales.
7. El sistema de gestión de derechos (10; 100) de la reivindicación 1, donde dicho al menos único elemento es una pluralidad de elementos de contenido protegido.
8. El sistema de gestión de derechos (10; 100) de cualquiera de las reivindicaciones 1 a 5, donde dicho punto de distribución está adaptado para preempaquetar dicha licencia (52; 116) de dicho dispositivo de licencia (50; 110) con dicho al menos único elemento para cada usuario en dicha lista de abonos.
9. El sistema de gestión de derechos (10; 100) de la reivindicación 8, donde dicho punto de distribución está adaptado además para contar el número de elementos a los que accede dicho al menos único usuario.
10. El sistema de gestión de derechos (10; 100) de la reivindicación 9, donde dicho dispositivo gestor de abonos (120) está adaptado además para quitar dicho al menos único usuario de dicha lista de abonos cuando dicho al menos único usuario accede a un número predeterminado de elementos.

11. El sistema de gestión de derechos (10; 100) de cualquiera de las reivindicaciones 1 a 10, donde dicho punto de distribución es una aplicación de escaparate en línea.

12. El sistema de gestión de derechos (10; 100) de cualquiera de las reivindicaciones 1 a 11, donde dicho dispositivo gestor de abonos (120) también incluye un directorio de servidor de correo.

13. Un método para gestionar el uso de elementos que tienen derechos de uso asociados, siendo dichos elementos protegidos e incluyendo dicho método los pasos de: proporcionar un paquete de software (103) a un dispositivo de cliente (30; 106) de al menos un usuario abonado, aplicando dicho paquete de software (103) derechos de uso para controlar el uso de dichos elementos y teniendo un par de claves pública-privada asociado con dicho al menos único usuario abonado; concediéndose dicho paquete de software (103) a dicho dispositivo cliente (30; 106) para permitir a dicho al menos un usuario abonado usar dichos elementos, estando asociado dicho al menos un usuario abonado con dicho dispositivo cliente (30; 106); proporcionar un componente de cliente (60) conteniendo un motor para examinar o presentar elementos protegidos a dicho dispositivo de cliente (30; 106), instalándose dicho componente de cliente en el dispositivo de cliente (30; 106) después de la recepción en el dispositivo de usuario (30; 106); siendo dicho componente de cliente (60) para interpretar dichas licencias (52); almacenar, por un dispositivo gestor de abonos (120), la clave pública de dicho par de claves pública-privada asociado con dicho al menos único usuario abonado en una lista de abonos correspondiente a dicho al menos único elemento; teniendo dicha lista de abonos claves públicas asociadas con usuarios abonados; recibir (506), por un punto de distribución (128), una petición de dicho al menos único usuario abonado para acceder a dicho al menos único elemento; pedir, por dicho punto de distribución (128), la licencia (52; 116) a un dispositivo de licencia (50; 110); donde la petición de licencia de dicho punto de distribución (128) incluye una lista de usuarios y sus claves públicas respectivas y una ID de contenido para la que se han de conceder las licencias; conceder, para cada usuario en la petición de licencia de dicho punto de distribución, una licencia (52; 116) en base a la identidad del usuario abonado (114); verificando que dicho usuario abonado que pide acceso a dicho al menos único elemento, figura en dicha lista de abonos verificando que la clave pública asociada con dicho usuario está en dicha lista de abonos antes de conceder dicha licencia (52; 116); y conceder, por dicho dispositivo de licencia (50; 110), la licencia (52; 116) que otorga derechos de uso a dicho usuario abonado para usar dicho al menos único elemento si dicha clave pública asociada con dicho usuario está en dicha lista de abonos; recibir, por dicho punto de distribución (128), la licencia (52; 116) de un dispositivo de licencia (50; 110); pre-empaquetar, por dicho punto de distribución (128), la licencia recibida (52; 116) con dicho al menos único elemento; y entregar o poner a disposición, por dicho punto de distribución (128), dicha licencia pre-empaquetada (116') con dicho al menos único elemento a dicho dispositivo de usuario (30; 106) asociado con dicho usuario abonado (114); donde dicho al menos un elemento está encriptado o protegido de manera que dicha licencia y dicho paquete de software se requieren como un componente de seguridad para usar dicho al menos un elemento.

14. El método de la reivindicación 13, donde dicho al menos único elemento es una pluralidad de elementos de contenido protegido adaptados para que a ellos acceda dicho al menos único usuario.

15. El método de la reivindicación 14, donde dicho al menos único usuario son múltiples usuarios e incluyendo además el paso de conceder una pluralidad de licencias (52; 116) que otorgan a cada uno de dichos usuarios múltiples derechos de uso de dicha pluralidad de elementos de contenido protegido.

16. El método de la reivindicación 15, incluyendo además el paso de verificar que cada uno de dichos múltiples usos se enumera en dicha lista de abonos antes de conceder cada licencia (52; 116) que otorga derecho de uso de dicha pluralidad de contenidos protegidos.

17. El método de la reivindicación 14, incluyendo además el paso de contar el número de elementos de contenido protegido usados por cada uno de dichos múltiples usuarios.

18. El método de la reivindicación 17, incluyendo además el paso de quitar dicho mecanismo de identificación asociado con un usuario cuando un número predeterminado de elementos de contenido protegido es utilizado por dicho usuario.

19. El método de la reivindicación 13, donde dicho mecanismo de identificación es una clave pública.

20. El método de la reivindicación 19, incluyendo además el paso de verificar que una clave pública de un usuario que pide acceso a un elemento particular de contenido protegido, figura en dicha lista de abonos antes de conceder una licencia (52; 116) que otorga a ese usuario derechos de uso de dicho elemento particular de contenido protegido.

21. El método de la reivindicación 13, incluyendo además el paso de preempaquetar dicha licencia concedida (52; 116) juntamente con dicho al menos único elemento para cada usuario en la lista de abonos.

22. El método de cualquiera de las reivindicaciones 13 a 21, siendo además el método para abonar un usuario para acceder a un elemento protegido, incluyendo además dicho método: conceder una clave privada y una clave pública a los usuarios; añadir la clave pública de los usuarios a la lista de abonos correspondiente a elementos de contenido

protegido; y empaquetar la licencia (52; 116) a uno de los elementos de contenido protegido después de la recepción de una petición de uno de los elementos de contenido protegido y la verificación de que la clave pública de un usuario que hace la petición es una clave pública que está en la lista de abonos.

Fig. 1

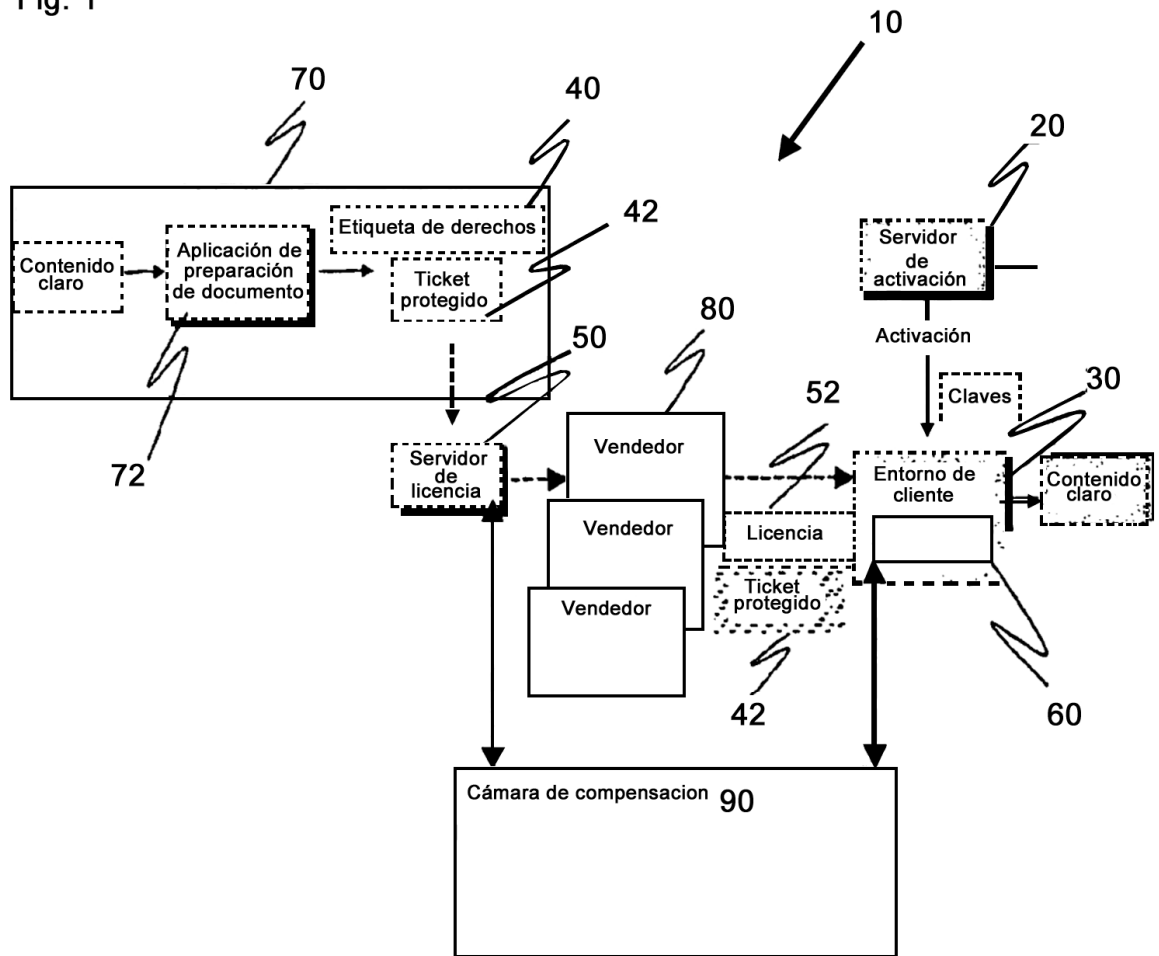


Fig. 2

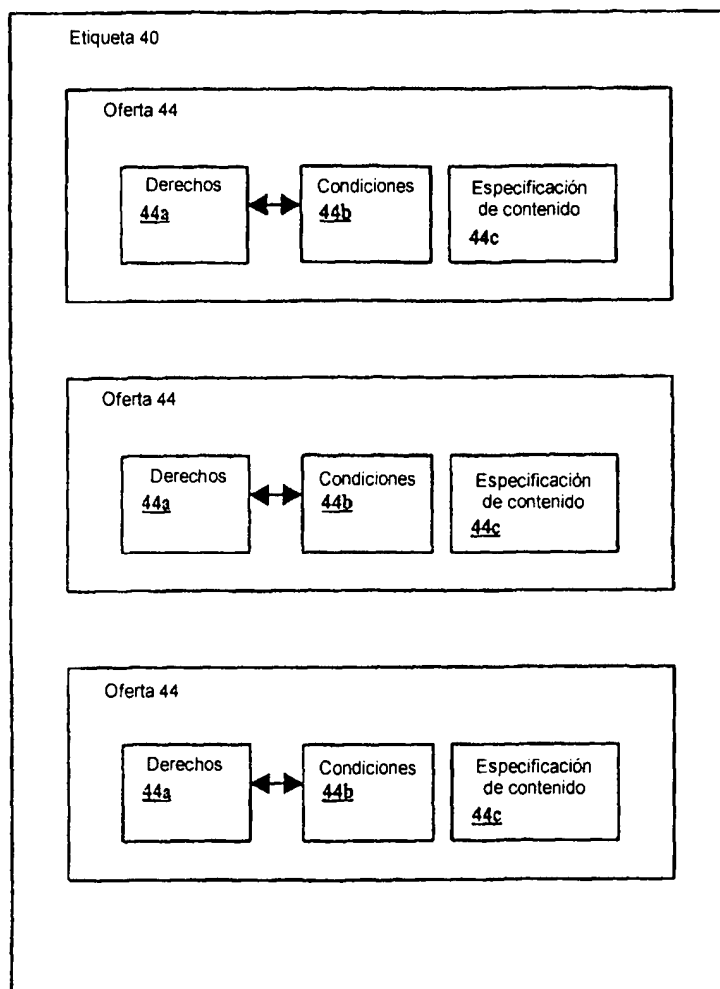


Fig. 3

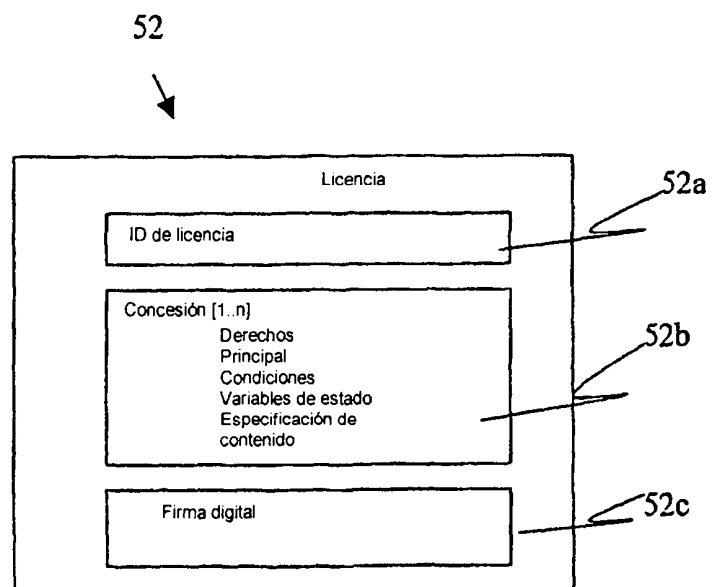


Fig.4

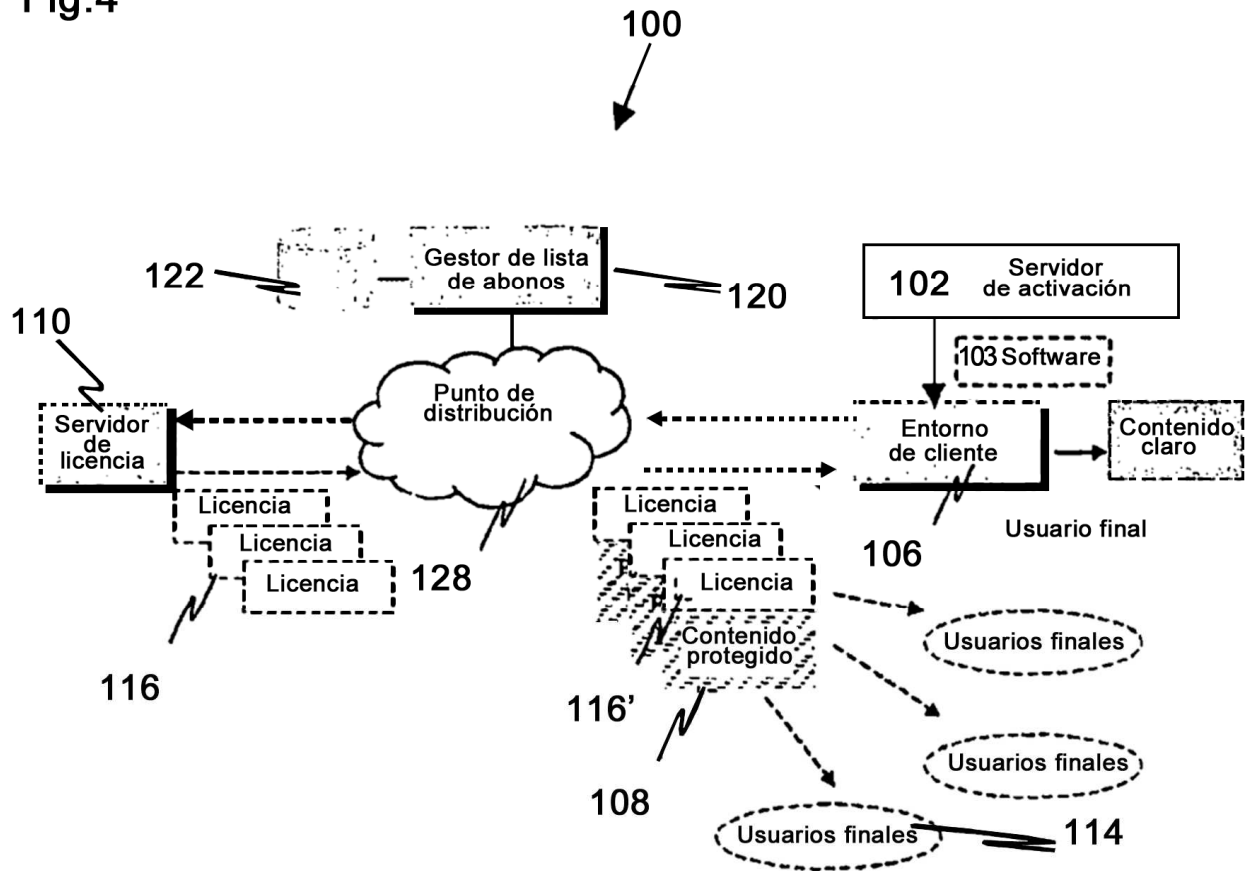


Fig. 5

