(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 616 250**

(51) Int. CI.:

G06F 1/00 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **13.12.2000 E 04026831 (0)**

(97) Fecha y número de publicación de la concesión europea: **23.11.2016 EP 1515214**

(54) Título: **Sistema y procedimiento para acceder a contenido protegido en una arquitectura de gestión de derechos**

(30) Prioridad:

17.12.1999 US 172318 P
17.12.1999 US 172319 P
27.06.2000 US 604946

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
12.06.2017

(73) Titular/es:

MICROSOFT TECHNOLOGY LICENSING, LLC (100.0%)
One Microsoft Way
Redmond, WA 98052, US

(72) Inventor/es:

DEMELLO, MARKO A.;
KRISHNASWAMY, VINAY y
MANFERDELLI, JOHN L.

(74) Agente/Representante:

CARPINTERO LÓPEZ, Mario

Aviso: En el plazo de nueve meses a contar desde la fecha de publicación en el Boletín Europeo de Patentes, de la mención de concesión de la patente europea, cualquier persona podrá oponerse ante la Oficina Europea de Patentes a la patente concedida. La oposición deberá formularse por escrito y estar motivada; sólo se considerará como formulada una vez que se haya realizado el pago de la tasa de oposición (art. 99.1 del Convenio sobre Concesión de Patentes Europeas).

DESCRIPCIÓN

Sistema y procedimiento para acceder a contenido protegido en una arquitectura de gestión de derechos

Referencia cruzada a casos relacionados

Esta solicitud reivindica el beneficio de la Solicitud Provisional de Estados Unidos N.º 60/172.319 titulada “System and Method for Digital Rights Management”, y la Solicitud Provisional de Estados Unidos N.º 60/172.318 titulada “System for Distributing Content Having Multinivel Security Protection”, ambas presentadas el 17 de diciembre de 1999.

Campo de la invención

La presente invención se refiere en general a distribución de contenido electrónico, y, más particularmente, a sistemas y procedimientos para acceder a contenido protegido en una arquitectura de gestión de derechos.

Antecedentes de la invención

A medida que ha aumentado la disponibilidad y uso de ordenadores y dispositivos electrónicos del tamaño de la palma de la mano, se ha hecho común que los documentos se transmitan y vean electrónicamente. Con mejoras en la velocidad y facilidad de la comunicación a través de infraestructuras tales como internet, existe un enorme control para proporcionar servicios y contenido mejorados a los dispositivos. Ejemplos de servicios y contenido que pueden proporcionarse son trabajos de autor, tales como libros u otro material textual. La distribución electrónica de documentos de texto es tanto más rápida como más barata que la distribución convencional de copias en papel. El mismo principio se aplica a contenido no de texto, tal como audio y vídeo: la distribución electrónica de tal contenido es generalmente más rápida y más barata que la entrega de tal contenido en medios convencionales (por ejemplo, cinta magnética o disco óptico). Sin embargo, el bajo coste e instantaneidad de la distribución electrónica, en combinación con la facilidad de copiar contenido electrónico, es contrario a la distribución controlada de una manera que proteja los derechos de los propietarios de los trabajos distribuidos.

Una vez que se transmite un documento electrónico a una parte, puede copiarse y distribuirse fácilmente a otros sin autorización por el propietario de los derechos en el documento electrónico o, en ocasiones, incluso sin el conocimiento del propietario. Este tipo de distribución de documentos ilícita puede privar al autor o al proveedor de contenido de regalías y/o ingresos. Un problema con muchos esquemas de entrega actuales es que no hacen provisiones para proteger derechos de propiedad. Otros sistemas intentan proteger derechos de propiedad, pero sin embargo, son complicados e inflexibles y hacen la visualización/lectura de los trabajos de autor (o presentan de otra manera los trabajos de autor, en el caso de contenido no de texto tal como música, vídeo, etc.) difíciles para el comprador.

Por lo tanto, en vista de lo anterior, existe una necesidad de un sistema de gestión de derechos digitales mejorado que permita la entrega de trabajos electrónicos a compradores de una manera que proteja los derechos de propiedad, mientras que también sea flexible y fácil de usar. Existe también una necesidad para que el sistema proporcione niveles flexibles de protección de seguridad y sea operable en varias plataformas de cliente de manera que el contenido electrónico pueda verse/presentarse mediante su comprador en cada plataforma. El sistema de gestión de derechos digitales de la presente invención proporciona ventajosamente soluciones a los problemas anteriores que protege los derechos de la propiedad intelectual de los propietarios de contenido y permite a los autores u otros propietarios de contenido ser compensados por sus esfuerzos creativos, mientras asegura que los compradores no se vean sobrecargados por el mecanismo de protección.

El documento US 5.883.955 describe un sistema en línea basado en ordenador para demostrar programas de software a un comprador potencial. Cuando un usuario solicita comprar información digital y proporciona cualquier información requerida tal como un número de tarjeta de crédito, el sistema distribuye una copia desbloqueada de la información digital al usuario. El sistema en línea puede interconectarse a redes existentes o servicios en línea. Los usuarios informáticos pueden descargar información desde redes tales como internet. Si el uso es en línea entonces el sistema descarga los paquetes de software que contienen programas encriptados a muestrearse o usa el fichero y monta el volumen virtual. Se describe que recibir un programa de software a demostrarse comprende significar la etapa de recibir el programa de software en un estado encriptado, y se describe habilitar el programa de software para ejecución que comprende la etapa de desencriptar el programa de software encriptado.

Sumario de la invención

Es el objeto de la invención proporcionar un procedimiento y sistema informático mejorados para soportar un sistema de distribución de contenido.

Este objeto se resuelve mediante la invención de acuerdo con las reivindicaciones independientes.

Se especifican realizaciones preferidas en las reivindicaciones dependientes.

Se proporciona una arquitectura para un cliente de presentación de contenido en un sistema de gestión de derechos

digitales (“DRM”). La arquitectura incluye una aplicación de presentación (por ejemplo, una aplicación de visualización de texto o “lector”) que presenta contenido protegido mediante el sistema de DRM. La arquitectura incluye también diversas características de seguridad que protegen frente a distribución no autorizada o uso del contenido protegido, así como componentes de software que navegan por las características de seguridad para permitir que el contenido se presente en un entorno de cliente apropiado.

De acuerdo con la arquitectura proporcionada, el contenido puede protegerse en una pluralidad de niveles, que incluyen: sin protección, sellado de origen, sellado individualmente (o “inscrito”), firmado de origen, y completamente individualizado (o “exclusivo de propietario”). El contenido “sin protección” se distribuye en un formato desencriptado. El contenido de “sellado de origen” y “sellado individualmente” está encriptado y agrupado con una clave criptográfica (la “clave de contenido”) que está sellada criptográficamente con ciertos datos de gestión de derechos asociados con el contenido, de manera que la clave no pueda recuperarse si se han modificado los datos de gestión de derechos. La distinción entre sellado de “origen” e “individual” es que el contenido “sellado individualmente” incluye en los datos de gestión de derechos información pertinente para el propietario legítimo (por ejemplo, el nombre del propietario, número de tarjeta de crédito, número de recibo o ID de transacción para la transacción de compra, etc.), de manera que esta información no puede eliminarse de una copia en funcionamiento del contenido, permitiendo de esta manera la detección de distribuidores no autorizados. El tipo de información particular incluida se determina mediante el vendedor minorista de la copia. El contenido “firmado” está firmado criptográficamente de manera que la aplicación de presentación puede verificar su autenticidad, o la autenticidad de su canal de distribución. El contenido “completamente individualizado” es contenido encriptado proporcionado con una clave de desencriptación que no se ha sellado simplemente con la información de gestión de derechos, sino también se ha encriptado de manera que no puede accederse en ausencia de un “repositorio seguro” y “certificado de activación”, que se emiten únicamente a un cliente o conjunto de clientes particulares, limitando de esta manera el uso de tal contenido a un número finito de instalaciones. El contenido “completamente individualizado” también incluye una licencia, que especifica los derechos que el usuario puede ejercer con respecto al contenido.

En una realización de la invención, el cliente se usa para leer libros o texto, que se distribuyen al cliente en un fichero que tiene protección como se ha descrito anteriormente. Preferentemente, el software de cliente y los datos relacionados con la protección y uso del contenido incluyen: la aplicación de presentación (denominada el “lector” en el caso donde el contexto sea texto); un componente de “gestión” que realiza el desellado del contenido protegido y ciertas otras funciones criptográficas; un objeto de software que proporciona a los distribuidores de contenido información tal como el estado de la instalación y/o de la “activación” de la aplicación de lector, así como información acerca del certificado de “activación” que es necesario por el distribuidor para preparar contenido “completamente individualizado” cuya capacidad de desencriptación está limitada a cierto conjunto de lectores; y un objeto de software de “activación” que realiza la función de obtener un repositorio seguro y certificado de activación para instalación en el cliente. Preferentemente, el objeto de software de activación se realiza como un control ACTIVEX, y el objeto que proporciona información a los sitios de distribución de contenido se realiza como un ACTIVEX y/o extensión de explorador encapsulada en una o más funciones de Java script. Adicionalmente, se prefiere que el objeto de gestión sea operable mediante la aplicación del lector a través de una API expuesta a la aplicación de lector.

Preferentemente, la clave de contenido de contenido completamente individualizado está encriptada de acuerdo con un par de claves pública/privada asociadas con un certificado de activación particular, y puede proporcionarse una copia del certificado de activación a diversos dispositivos de cliente de propiedad o usados por una persona particular (o “persona”), de manera que una persona pueda leer el mismo contenido “completamente individualizado” en varios dispositivos de propiedad o usados por esa persona, mientras que otras personas que posean dispositivos similares no puedan leer el mismo contenido “completamente individualizado” puesto que el certificado de activación necesario no se emitirá para aquellas personas, limitando de esta manera la divulgación de contenido completamente individualizado.

Otras características de la invención se describen a continuación.

Breve descripción de los dibujos

El anterior resumen, así como la siguiente descripción detallada, se entienden mejor cuando se leen en conjunto con los dibujos adjuntos. Para el fin de ilustrar la invención, números de referencias similares representan partes similares a lo largo de todas las varias vistas de los dibujos, se entiende, sin embargo, que la invención no está limitada a los procedimientos específicos e instrumentalidades desveladas. En los dibujos:

La Figura 1 es un diagrama de bloques que muestra un entorno informático ejemplar en el que pueden implementarse aspectos de la presente invención;
La Figura 2 es un diagrama de bloques de una primera realización de una arquitectura de cliente que implementa aspectos de un sistema de gestión de derechos digitales de acuerdo con la invención;
La Figura 3 es un diagrama de bloques de una segunda realización de una arquitectura de cliente que implementa aspectos de un sistema de gestión de derechos digitales de acuerdo con la invención;
La Figura 4 es un formato de fichero de título de libro electrónico (eBook) ejemplar;
La Figura 5 es un diagrama de flujo que ilustra un procedimiento de activación de lector; y

La Figura 6 es un diagrama de flujo que ilustra procedimientos ejemplares para seleccionar, obtener y leer un libro electrónico usando un sistema de gestión de derechos digitales de acuerdo con la invención.

Descripción detallada de la invención

La presente invención se refiere a un sistema para procesamiento y entrega de contenido electrónico en el que el contenido electrónico puede protegerse a múltiples niveles. Se describe una realización preferida de la invención, que se refiere al procesamiento y entrega de libros electrónicos, sin embargo, la invención no está limitada a libros electrónicos y puede incluir todo contenido digital tal como vídeo, audio, ejecutables de software, datos, etc.

Vista general

El éxito de la industria del libro electrónico sin duda requerirá proporcionar al público existente que compra libros con una experiencia atractiva, segura y familiar para obtener todos los tipos de material textual. Este material puede incluir material "gratis" o de bajo coste que requiere poca protección de copia, a títulos de libro electrónico de "calidad especial" (en el presente documento "libros electrónicos") que requieren protección de derechos integral. Para habilitar una transición suave desde la distribución actual y el modelo de venta minorista para libros impresos a un sistema de distribución electrónico, debe existir una infraestructura para asegurar un alto nivel de protección de copia para aquellas publicaciones que lo demandan, mientras soporta la distribución de títulos que requieran niveles de protección inferiores.

Los sistemas de Gestión de Derechos Digitales (DRM) y de Servidor de Bienes Digitales (DAS) de la presente invención proporcionan ventajosamente una infraestructura de este tipo. La presente invención hace comprar un libro electrónico más deseable que "robar" (por ejemplo, hacer una copia no autorizada de) un libro electrónico. El sistema de DRM no intrusivo minimiza el riesgo de piratería, mientras aumenta la probabilidad de que cualquier piratería se compense por ventas/distribución aumentada de libros en forma de libros electrónicos. Además, la presente invención proporciona a los vendedores minoristas con un sistema que puede desplegarse rápidamente a bajo coste.

Los usuarios principales del sistema de DRM son editores y vendedores minoristas, que usan y/o despliegan el sistema de DRM para asegurar la legitimidad del contenido vendido así como la protección de copia. Los usuarios ejemplares del sistema de DRM pueden ser el editor tradicional, el editor "avanzado", y el "autor hambriento". El editor tradicional es probable que esté preocupado acerca de perder beneficios de su operación de publicación de libro impreso a la piratería de libro electrónico. El editor avanzado no está necesariamente preocupado por incidentes aislados de piratería y puede apreciar que el comercio de los libros electrónicos será más satisfactorio en un sistema donde los consumidores desarrollen hábitos de compra. Mientras tanto, el autor hambriento, que le gustaría recolectar dinero por la venta de sus trabajos, está más interesado en atribución (por ejemplo, que el nombre del autor esté unido permanentemente al trabajo).

Como se describirá en mayor detalle a continuación, el sistema de DRM de la presente invención consigue sus objetivos protegiendo trabajos, mientras habilita su uso legítimo por los consumidores, soportando diversos "niveles" de protección. En el nivel más bajo ("Nivel 1"), el origen de contenido y/o el proveedor pueden elegir no protección mediante libros electrónicos no firmados y no sellados (texto sin cifrar) que no incluyen una licencia. Un siguiente nivel de protección ("Nivel 2") es "sellado de origen", que significa que el contenido se ha encriptado y sellado con una clave, donde el sello se hace usando un troceo criptográfico de los metadatos del título del libro electrónico (véase a continuación) y la clave es necesaria para desencriptar el contenido. El sellado de origen protege frente a manipulación con el contenido o sus metadatos adjuntos después de que el título se ha sellado, puesto que cualquier cambio a los metadatos presentará el título no usable; sin embargo, el sellado de origen no garantiza autenticidad de la copia del título (es decir, el sellado de origen no proporciona un mecanismo para distinguir copias legítimas de copias no autorizadas). En el caso del "autor hambriento", el nombre del autor puede incluirse en los metadatos para unión permanente al contenido, satisfaciendo de esta manera el objetivo de atribución del "autor hambriento". Un siguiente nivel de protección ("Nivel 3") es "sellado individualmente" (o "inscrito"). Un título "sellado individualmente" es un libro electrónico cuyos metadatos incluyen información relacionada con el comprador legítimo (por ejemplo, el nombre del usuario o el número de tarjeta de crédito, el ID de transacción o número de recibo de la transacción de compra, etc.), de manera que esta información está unida criptográficamente al contenido cuando se sella el título. Este nivel de protección desalienta a las personas de distribuir copias del título, puesto que sería fácil de detectar el origen de una copia no autorizada (y cualquier cambio a los metadatos, incluyendo la información relacionada con el comprador, haría imposible, o al menos improbable, que la clave de desencriptación necesaria pudiera desellarse).

El siguiente nivel de protección ("Nivel 4") es "firmado de origen". Los libros electrónicos firmados de origen son títulos que pueden autenticarse por un "lector" (que, como se analiza más particularmente a continuación, es una aplicación de usuario que habilita la lectura de libros electrónicos en un dispositivo informático, tal como un PC, un portátil, un Asistente Digital Personal (PDA), PocketPC, o un dispositivo de lectura construido para tal fin). La autenticidad puede definirse preferentemente en tres diversidades: "herramienta firmada", que garantiza que el título de libro electrónico se generó por una conversión confiable y herramienta de encriptación; "propietario firmado" que es un libro electrónico de herramienta firmada que también garantiza la autenticidad del contenido en la copia (por

ejemplo, el propietario puede ser el autor u otro titular de los derechos de autor); y “proveedor firmado”, que es un libro electrónico de herramienta firmada que confirma a la autenticidad de su proveedor (por ejemplo, el editor o vendedor minorista del contenido). La “herramienta”, el propietario y el proveedor puede tener cada uno su propio par de claves asimétricas para facilitar la creación y validación de firmas digitales de la información. Un título puede estar tanto firmado de proveedor como firmado de origen, que facilita la autenticación del canal de distribución del título (por ejemplo, a través de una cadena de firma en la copia). El nivel más fuerte de protección es “completamente individualizado” o “exclusivo de propietario” (“Nivel 5”). Los títulos “completamente individualizados” únicamente pueden abrirse mediante aplicaciones de lector autenticadas que están “activadas” para un usuario particular, protegiendo de esta manera contra la portabilidad de un título de un lector (o lectores) de una persona a un lector que no está registrado para esa persona. Para que el lector de la presente invención abra un título protegido en el Nivel 5, el lector debe estar “activado” (es decir, el dispositivo en el que el reside el lector debe tener un certificado de activación para una persona particular, y un repositorio seguro). El procedimiento de activación se describirá en mayor detalle a continuación con referencia a la Figura 5.

Los sistemas de la presente invención definen también una arquitectura para compartir información entre un lector, un proveedor de contenido y un origen de contenido, cómo se usa esa información para “sellar” títulos en los diversos niveles, y cómo debe estructurarse esa información. La disponibilidad de estas elecciones habilitará a los orígenes de contenido tomar y elegir qué contenido se venderá a qué usuarios y usar qué protección (si la hubiera). La información particular puede usarse para firmar y/o sellar títulos para uso mediante un lector, y un lector compatible (que, en el caso del nivel 5, puede ser un lector activado para una persona particular) puede desellar el título y habilitar la lectura del libro electrónico.

Arquitectura de sistema

Como se muestra en la Figura 1, un sistema ejemplar para implementar la invención incluye un dispositivo informático de fin general en forma de un ordenador personal o servidor 20 de red o similar, que incluye una unidad 21 de procesamiento, una memoria 22 de sistema, y un bus 23 de sistema que acopla diversos componentes de sistema incluyendo la memoria 22 de sistema a la unidad 21 de procesamiento. El bus 23 de sistema puede ser cualquiera de varios tipos de estructuras de bus incluyendo un bus de memoria o controlador de memoria, un bus de periféricos y un bus local usando cualquiera de una diversidad de arquitecturas de bus. La memoria de sistema incluye memoria 24 de solo lectura (ROM) y memoria 25 de acceso aleatorio (RAM). Un sistema 26 básico de entrada/salida (BIOS), que contiene las rutinas básicas que ayudan a transferir información entre elementos en el ordenador 20 personal, tal como durante el arranque, se almacena en la ROM 24. El ordenador personal o servidor 20 de red puede incluir adicionalmente una unidad 27 de disco duro para leer desde y escribir en un disco duro, no mostrado, una unidad 28 de disco magnético para leer desde o escribir en un disco 29 magnético extraíble, y una unidad 30 de disco óptico para leer o escribir en un disco 31 óptico extraíble tal como un CD-ROM u otro medio óptico. La unidad 27 de disco duro, la unidad 28 de disco magnético y la unidad 30 de disco óptico están conectadas al bus 23 de sistema mediante una interfaz 32 de unidad de disco duro, una interfaz 33 de unidad de disco magnético, y una interfaz 34 de unidad óptica, respectivamente. Las unidades y sus medios legibles por ordenador asociados proporcionan almacenamiento no volátil de instrucciones legibles por ordenador, estructuras de datos, módulos de programa y otros datos para el ordenador personal o servidor 20 de red. Aunque el entorno ejemplar descrito en el presente documento emplea un disco duro, un disco 29 magnético extraíble y un disco 31 óptico extraíble, debería apreciarse por el experto en la materia que otros tipos de medios legibles por ordenador que pueden almacenar datos que son accesibles por un ordenador, tales como cintas magnéticas, tarjetas de memoria flash, discos de vídeo digital, cartuchos Bernoulli, memorias de acceso aleatorio (RAM), memorias de solo lectura (ROM) y similares pueden usarse también en el entorno de operación ejemplar.

Un número de módulos de programa pueden almacenarse en el disco duro, el disco 29 magnético, el disco 31 óptico, la ROM 24 o la RAM 25, incluyendo un sistema 35 operativo (por ejemplo, Windows® 2000, Windows NT®, o Windows 95/98), uno o más programas 36 de aplicación, otros módulos 37 de programa y datos 38 de programa. Un usuario puede introducir comandos e información en el ordenador 20 personal a través de los dispositivos de entrada tales como un teclado 40 y dispositivo apuntador 42. Otros dispositivos de entrada (no mostrados) pueden incluir un micrófono, palanca de mando, control de juegos, disco satélite, escáner o similares. Estos y otros dispositivos de entrada a menudo están conectados a la unidad 21 de procesamiento a través de una interfaz 46 de puerto serie que está acoplada al bus 23 de sistema, pero pueden estar conectados mediante otras interfaces, tal como un puerto paralelo, puerto de juegos, bus serie universal (USB), o un puerto en serie a alta velocidad 1394. Un monitor 47 u otro tipo de dispositivo de visualización también está conectado al bus 23 de sistema mediante una interfaz, tal como un adaptador 48 de vídeo. Además del monitor 47, los ordenadores personales típicamente incluyen otros dispositivos de salida periféricos (no mostrados), tales como altavoces e impresoras.

El ordenador personal o servidor 20 de red puede operar en un entorno en red usando conexiones lógicas a uno o más ordenadores remotos, tal como un ordenador 49 remoto. El ordenador 49 remoto puede ser otro ordenador personal, otro servidor de red, un encaminador, un PC de red, un dispositivo de pares u otro nodo de red común, y típicamente incluye muchos o todos los elementos anteriormente descritos con relación al ordenador 20 personal, aunque únicamente se ha ilustrado un dispositivo 50 de almacenamiento de memoria en la Figura 2. Las conexiones lógicas representadas en la Figura 2 incluyen una red 51 de área local (LAN) y una red 52 de área extensa (WAN). Tales entornos de interconexión de red son habituales en oficinas, redes informáticas a nivel de empresa, intranets e

internet.

Cuando se usa en un entorno de interconexión de red LAN, el ordenador personal o servidor 20 de red está conectado a la red 51 local a través de una interfaz o adaptador 53 de red. Cuando se usa en un entorno de interconexión de red WAN, el ordenador personal o servidor 20 de red típicamente incluye un módem 54 u otros medios para establecer comunicaciones a través de la red 52 de área extensa, tal como internet. El módem 54, que puede ser interno o externo, está conectado al bus 23 de sistema mediante la interfaz 46 de puerto serie. En un entorno en red, los módulos de programa con relación al ordenador personal o servidor 20 de red, o porciones de los mismos, pueden almacenarse en el dispositivo 50 de almacenamiento de memoria remoto. Se apreciará que las conexiones de red mostradas son ejemplares y que pueden usarse otros medios para establecer un enlace de comunicaciones entre los ordenadores.

Arquitectura de cliente

Haciendo referencia ahora a la Figura 2, se ilustra una primera arquitectura 90 de cliente ejemplar de acuerdo con la presente invención. La arquitectura 90 de cliente puede implementarse en el ordenador 20 personal de la Figura 1 u otro dispositivo informático apropiado, tal como un ordenador del tamaño de la palma de la mano, ordenador portátil, o dispositivo cerrado que esté construido para tal fin para leer títulos de libro electrónico. La arquitectura 90 de cliente incluye un intérprete de comandos 92 de cliente (o “lector 92”) para leer los títulos 10 de libro electrónico y un explorador 102 web (por ejemplo, el explorador MICROSOFT® INTERNET EXPLORER) para entrar en contacto con sitios de vendedor minorista/distribuidor. Se proporciona una transformación criptográfica, que puede ser una extensión para un Sistema de Almacenamiento de Tecnología de Información (ITSS) 5.2 96. La transformación criptográfica es un componente de software que desellará la clave de contenido y desencriptará el flujo de contenido que provenga del fichero de libro electrónico o “fichero LIT” 10 (mostrado en la Figura 4). La transformación criptográfica se implementa preferentemente como una extensión al código ITSS 96 existente que se está usando mediante el lector 92 para ficheros 10 LIT. Esta extensión se instancia cada vez que se accede a contenido encriptado. Se proporciona una API 94 exlibris que devuelve el nombre del comprador (u otra información relacionada con el comprador) desde el flujo 14C exlibris criptográficamente troceado dentro del objeto 14 de almacenamiento de DRM de cada título 10 (por ejemplo, en el caso de títulos sellados individualmente que incluyen el nombre del comparador u otra información de identificación en sus metadatos). La cadena devuelta por esta función puede usarse en la página 100 de cubierta del libro para identificar el propietario legítimo del título 10; un ejemplo, en el que la cadena es el nombre del usuario, se representa en la Figura 2. Si el usuario hace clic en el nombre visualizado (o toca, en el caso de dispositivos de pantalla táctil) o en un aviso/icono de derechos de autor en la página de cubierta, puede presentarse un cuadro de diálogo que destaca la naturaleza de los derechos de autor de la publicación. El almacenamiento 98 local es preferentemente un directorio o carpeta donde pueden almacenarse libros electrónicos. (Como se analiza a continuación en relación con la Figura 4, el libro electrónico 10 es un fichero que contiene el contenido del libro, así como otra información). Por ejemplo, cuando la arquitectura 90 se implementa en un dispositivo que opera bajo uno de los sistemas operativos MICROSOFT WINDOWS, el almacenamiento 98 local puede ser simplemente un directorio denominado “C:\MyLibrary”. El explorador 102 es un programa de exploración típico (tal como el explorador MICROSOFT INTERNET EXPLORER o el explorador NETSCAPE NAVIGATOR); se usa para entrar en contacto con sitios de venta minorista que venden libros electrónicos y para participar en transacciones con estos sitios. En algunos casos, el lector 92 puede tener una característica de “biblioteca integrada” que entra en contacto con sitios de venta minorista y facilita hacer compras sin el uso de una aplicación 120 de exploración general.

Haciendo referencia ahora a la Figura 3, se ilustra una segunda arquitectura 90’ de cliente ejemplar. En la segunda arquitectura de cliente, números de referencia similares representan elementos similares como en la primera arquitectura de cliente, y por lo tanto las descripciones de estos elementos similares no se repiten a continuación. El gestor 80 de DRM es un componente que expone un conjunto de API internas para el lector 92, que gestiona la autenticación de aplicaciones que solicitan acceso a los ficheros LIT encriptados, además de llevar a cabo desencriptación de contenido, desellado de las claves, devolución de una cadena exlibris (por ejemplo, el nombre del usuario para visualización en el caso de, por ejemplo, títulos de nivel 3 o de nivel 5), etc. Por ejemplo, el código para el lector 92 puede incluir una llamada de interfaz que es parte de la API, donde la llamada invoca instrucciones ejecutables por ordenador para llevar a cabo una de las funciones anteriormente listadas. Las instrucciones ejecutables por ordenador pueden incorporarse en un objeto COM y/o una biblioteca de enlace dinámico (DLL) para uso mediante el lector 92. Pueden proporcionarse diferentes versiones del objeto COM y/o de la DLL para adaptar las actualizaciones a las tecnologías (es decir, para permitir al lector 92 funcionar de manera transparente, a través de una API constante, con diversas tecnologías de DRM diferentes, algunas de las cuales pueden incluso no haberse desarrollado en el momento en el que se creó el código para el lector 92). En un ejemplo, el desarrollador/administrador de la arquitectura 90’ puede proporcionar una especificación o descripción de interfaz (por ejemplo, un conjunto de nombres de procedimientos/etiquetas para la API) al desarrollador del lector 92, y puede proporcionar a continuación una DLL u objeto COM (o sucesivas DLL y objetos COM) a los usuarios de la arquitectura 90’ de cliente. En otro ejemplo, el desarrollador/administrador de la arquitectura 90’ puede ser la misma entidad que proporciona el lector 92, y puede definir una API para que el gestor 80 de DRM facilite comunicación con los diversos componentes de la arquitectura 90’.

El repositorio 82 seguro es un ejecutable que se descarga durante el procedimiento de activación y habilita al lector

abrir libros electrónicos (ficheros LIT) completamente individualizados (nivel 5). El repositorio 82 seguro es preferentemente único (o sustancialmente único) para cada dispositivo informático en el que se implementa la arquitectura 90' (por ejemplo, un PC o dispositivo de lectura construido para tal fin). El repositorio 82 seguro mantiene una clave privada que se requiere para abrir títulos protegidos de nivel 5. El repositorio 82 seguro puede obtenerse durante el procedimiento de activación (descrito a continuación). En un ejemplo, el dispositivo informático en el que reside la arquitectura 90' carga (mediante una red, tal como la red 52) un ID de hardware a un "servidor de repositorio seguro" (no mostrado), donde el ID de hardware está basado en hardware asociado con el dispositivo informático (por ejemplo, mediante números de serie u otros números asociados con ese hardware) e identifica de manera inequívoca el dispositivo. El "servidor de repositorio seguro" puede a continuación descargar al dispositivo informático un repositorio seguro cuyo código está basado en, y cuya ejecución apropiada está vinculada preferentemente, al dispositivo informático en el que se implementa la arquitectura 90', cuando el repositorio seguro realiza funciones que incluyen aplicar una clave privada única que se usa en el procedimiento de desellar la clave de contenido, así como desencriptar el contenido. En una realización ejemplar, el contenido en un título de nivel 5 está encriptado con una clave simétrica, la clave simétrica está encriptada con una clave pública contenida en un certificado de activación, la clave simétrica encriptada está sellada con el título, y la clave privada del certificado de activación está contenida en el certificado de activación en una forma encriptada mediante la clave pública del repositorio 82 seguro. En este ejemplo, el repositorio 82 seguro desencripta la clave privada del certificado de activación usando la clave privada del repositorio 82 seguro, y a continuación la clave privada del certificado de activación se usa para desencriptar la clave simétrica. Un sistema y procedimiento para crear el repositorio 82 seguro se describen en el Expediente del Mandatario Número MSFT-0126, presentado concurrentemente con el presente e incorporado por referencia expresamente en su totalidad.

El control 84 ACTIVEX de activación es un componente usado por el dispositivo informático de cliente durante el procedimiento de activación (véase a continuación). Preferentemente, el control 84 ACTIVEX se usa mediante un explorador (por ejemplo, un explorador MICROSOFT INTERNET EXPLORER), que, a su vez, está alojado mediante el lector 92 (aunque el control 84 ACTIVEX podría funcionar también con un explorador independiente). El control 84 ACTIVEX de activación expone procedimientos que proporcionan la validación de servidores (por ejemplo, el "servidor o servidores de activación") a los que el lector 92 (o el dispositivo informático en el que reside) está conectado, cálculo del ID de hardware, descarga del repositorio 82 seguro (y certificados de activación asociados), y autenticación e instalación del ejecutable descargado. Por ejemplo, el lector 92 (u otro componente de software) puede contener instrucciones para detectar si el lector 92 ha sido activado y, si no ha sido activado, puede emitir una o más instrucciones para que el control 84 ACTIVEX de activación realice la activación, y estas instrucciones pueden incluir instrucciones para realizar los actos enumerados anteriormente.

El objeto 86 de comercio web se distribuye tanto como un control ACTIVEX y una extensión de NETSCAPE NAVIGATOR®. Puede usarse, mediante lenguaje de guiones del lado de cliente, por revendedores minoristas cuando venden copias completamente individualizadas (es decir, copias protegidas de Nivel 5). Este objeto 86 COM está preferentemente encapsulado mediante funciones de guion de lado de cliente que resumen los procedimientos reales y diferencias subyacentes entre la extensión y el control ACTIVEX. Los procedimientos clave proporcionados mediante el objeto 86 de comercio web y su interfaz adjunta son: detección de la instalación del lector 92, detección del estado de activación, lanzamiento del lector en el procedimiento de activación (véase, Figura 5), recuperación de ID de PASSPORT encriptado con el que se activó el lector, y recuperación de un (preferentemente encriptado) certificado de activación durante descarga de copias completamente individualizadas (protegidas de Nivel 5). Por ejemplo, un guion (tal como un Java script) puede distribuirse a los vendedores minoristas de libros electrónicos para inclusión en las páginas web del vendedor minorista. El guion puede exponer llamadas de función que implementan los procedimientos anteriormente enumerados, y el guion puede incluir código para determinar si se está ejecutando mediante un explorador MICROSOFT INTERNET EXPLORER o un explorador NETSCAPE NAVIGATOR, donde usa el control ACTIVEX en el primer caso y la extensión en el segundo caso. Un vendedor minorista puede transmitir de manera eficaz instrucciones a realizarse en el dispositivo informático de cliente transmitiendo el guion que define las llamadas de función junto con instrucciones de guion que invocan las funciones. Por ejemplo, un vendedor minorista puede desear detectar si el lector 92 está instalado en un dispositivo informático del cliente, por lo que el vendedor minorista puede transmitir al dispositivo cliente una página web que contiene el Java script que define la función para detectar si el lector 92 está instalado, junto con una instrucción para invocar esa instrucción. La propia función de detección puede incluir código para realizar la función de detección de cualquiera del control ACTIVEX o la extensión dependiendo de la marca del explorador en el que se esté ejecutando el guion. De esta manera, el explorador particular es transparente para el vendedor minorista, que puede crear una página web sencilla que realiza cualquiera de las funciones anteriormente enumeradas en cualquier explorador.

Estructura de fichero de libro electrónico

Haciendo referencia ahora a la Figura 4, se muestra una estructura de fichero de libro electrónico (o "LIT") ejemplar. El libro electrónico 10 contiene contenido 16, que es texto tal como un libro (o cualquier contenido electrónico, tal como audio, vídeo, etc.) que se ha encriptado mediante una clave (la "clave de contenido"), que ella misma ha sido encriptada y/o sellada. En una realización preferida, la clave es una clave 14A simétrica que se sella con un troceo criptográfico de metadatos 12 o, en el caso de títulos de nivel 5, con la clave pública del certificado de activación del usuario. Esta clave se almacena como un flujo separado en una sección de sub-almacenamiento del fichero del libro

electrónico (flujo 14A de almacenamiento 14 de DRM en la Figura 4) o, en el caso de títulos de nivel 5, en la licencia. (En el caso de títulos de nivel 5, en lugar de almacenar la clave de contenido como un flujo separado, el flujo 14A contiene una licencia, que es una construcción que define los derechos que el usuario puede ejercer tras la compra del título. En los títulos que tienen una licencia, la clave de contenido está contenida en la licencia). Incluido también en el almacenamiento 14 de DRM está el flujo 14B de origen, que puede incluir el nombre del editor (u otro origen de contenido), así como el flujo 14C exlibris, que, para títulos sellados individualmente (nivel 3 y/o nivel 5), incluye el nombre del consumidor según se proporciona mediante el vendedor minorista (que puede, por ejemplo, obtenerse como parte de la transacción comercial de comprar un libro electrónico 10, tal como desde la información de tarjeta de crédito del consumidor). El procedimiento para calcular el troceo criptográfico que encripta y/o sella la clave 14C simétrica (o el procedimiento para usar tal troceo criptográfico para sellar la clave) es preferentemente un "secreto" conocido únicamente para herramientas de preparación de contenido confiables y aplicaciones de presentación confiables. Usar un troceo de esta manera puede complicar/desalentar la manipulación de los metadatos 12 contenidos con el libro electrónico 10. Se observa que cualquier procedimiento puede usarse para "sellar" un libro electrónico, siempre que tal procedimiento proporcione alguna medida de resistencia a manipulación para el libro electrónico 10.

De acuerdo con la presente invención, los metadatos 12 pueden incluir una etiqueta de derechos de autor, que describe los derechos concedidos al usuario o comprador mediante el origen de contenido (por ejemplo, el editor). Cada vez que tal etiqueta esté presente, el lector 92 puede visualizar a un usuario el texto incluido en la etiqueta, por ejemplo cuando el usuario toca en el nombre visualizado en la página 100 de cubierta (mostrado en las Figuras 2 y 3) en el caso de copias selladas individualmente, o en el enlace de "Aviso de Derechos de Autor" (en el caso de copias selladas de origen con una etiqueta de derechos de autor), que puede presentarse también en la página 100 de cubierta. Si la etiqueta de derechos de autor no está incluida en los metadatos 12 por el origen de contenido, pero el título del libro electrónico se ha sellado individualmente (Nivel 3), la aplicación de lectura basándose en el sistema desvelado (por ejemplo, el lector 92) puede presentar un aviso de derechos de autor genérico como el siguiente mensaje o un mensaje similar: "Ninguna parte de esta publicación electrónica puede reproducirse, re-distribuirse, o retransmitirse en cualquier forma o por cualquier medio, electrónico, mecánico, impresión, fotocopiado, grabación o mediante cualquier almacenamiento de información y sistema de recuperación, sin consentimiento escrito a partir del editor". Se apreciará que el acto de visualizar un aviso de derechos de autor sirve para disuadir que los usuarios típicos intenten copiar sus libros electrónicos, y un aviso de este tipo puede visualizarse en cualquier punto durante la visualización de un libro electrónico cuando se considere ventajoso para recordar a los usuarios que están viendo material de propiedad.

Activar un lector

Como se ha indicado anteriormente, la activación habilita a un cliente lector comprar, descargar y visualizar títulos de libro electrónico completamente individualizados (es decir, nivel 5). Puesto que los ordenadores que ejecutan uno del sistema operativo MICROSOFT WINDOWS® (u otro sistema operativo de fin general) son esencialmente plataformas abiertas donde cualquier persona puede depurar un procedimiento de ejecución y crear "parches" (módulos de modificación de software) para piratear informáticamente la seguridad de cualquier aplicación, la necesidad de establecer una estructura de seguridad acerca del cliente lector es un prerrequisito para proporcionar verdadera protección/resistencia a copia. La "activación" es el procedimiento mediante el cual se establece esta estructura para el lector 92.

Se prefiere que el procedimiento de activación se realice usando una "autoridad de espacio de nombres", tal como MICROSOFT® PASSPORT™, como la base de datos de activación. El uso de PASSPORT™ permite ventajosamente la vinculación del certificado de activación del usuario a su persona. Como se usa en el presente documento, una "persona" es un identificador único que puede vincularse a un usuario y puede autenticarse de manera segura mediante un procedimiento fuera de banda - por ejemplo, un nombre de usuario y contraseña desde un explorador web para uso a través de una capa de conexión segura (SSL) es una realización de ejemplo de un procedimiento de este tipo. Al usar un esquema de "persona", un individuo puede leer títulos comprados en cualquier lector que se haya activado usando la "persona" bajo la que se compró el título. También, una vez activado, la información de activación puede ponerse a disposición de múltiples comerciantes para eliminar la necesidad de comunicaciones de servidor a servidor entre los comerciantes y la autoridad de activación, mientras se mitigan asuntos de privacidad.

El procedimiento mediante el cual se activa un lector se describirá ahora. Una vez que un usuario compra un dispositivo de lectura de libros electrónicos construido para tal fin, u obtiene software de lector para un PC (por ejemplo, mediante el CD-ROM 31, o descarga mediante una red 52 de área extensa tal como internet), se alienta al usuario a activar el lector la primera vez que se lanza el lector (por ejemplo, inmediatamente después de la configuración para la aplicación de portátil/sobremesa). Por ejemplo, cada vez que se lanza el lector, puede comprobar para ver si se ha activado (u otro objeto de software puede comprobar si el lector se ha activado). Si el lector no se ha activado, el lector presentará un cuadro de diálogo que recuerda al usuario que él o ella no podrá obtener títulos especiales que requieren individualización completa (es decir, protección de nivel 5). Un ejemplo de un recordatorio de este tipo es:

Enhorabuena por instalar Microsoft® Reader. Para habilitar a su lector para compra y descarga de títulos

especiales que se han asegurado para distribución, necesitará activarlo en línea.

El diálogo puede incluir botones para permitir al usuario activar el lector 92 (por ejemplo, el cuadro de diálogo puede visualizar dos botones marcados “activar lector ahora” y “activar lector más tarde”). Una “casilla de verificación” puede incluirse en el cuadro de diálogo con un mensaje tal como “Por favor no mostrarme este mensaje en el futuro”, que el usuario podría verificar si él o ella no estuviera interesado en obtener títulos de nivel 5, de modo que el lector dejaría de visualizar el mensaje de activación después de lanzar. Si el lector se ha activado anteriormente, se presentará el ID de PASSPORT o el ID de la persona del último usuario que activó el lector así como en una “pantalla de bienvenida”, tal como “Activado para <persona>”. El usuario puede activar también el lector desde cualquier sitio web de venta minorista, mientras hace compras con un explorador independiente. En este escenario, los comerciantes pueden aprovechar un procedimiento expuesto mediante el objeto 86 de comercio web del lector y API encapsuladora de guion asociado para presentar un enlace y/o botón que lanza el lector 92 como un procedimiento separado. Por ejemplo, un comerciante puede incluir en una página web una función de guion que lanza el lector 92 en su característica de activación, que a continuación guía al usuario a través de las etapas de activación, tal como si el usuario hubiera iniciado el lector y lanzado la característica de activación por sí mismo. (Como se ha indicado anteriormente, la función de guion puede realizar el lanzamiento usando un control ACTIVEX o una extensión de acuerdo con qué tipo de explorador se esté ejecutando). El comerciante puede incluir también en una página web una instrucción (usando el objeto 86 de comercio web y guion encapsulador asociado) para detectar en primer lugar si el lector 92 está activado, y lanzar el procedimiento de activación únicamente si el lector 92 no se ha activado previamente. En otro escenario, el lector 92 puede estar usando una característica de “biblioteca integrada” del lector (por ejemplo, una característica que permite al usuario hacer compras en diversos sitios web que venden libros electrónicos sin usar un explorador), y el procedimiento de activación puede lanzarse desde (o parte de) la característica de “biblioteca integrada” del lector 92.

Suponiendo que el usuario ha decidido activar el lector 92, el procedimiento de activación puede incluir las etapas ilustradas en la Figura 5. En la etapa 150, el cliente de lector abre la sección “biblioteca integrada” y conecta, mediante la Capa de Conexión Segura (SSL), a los servidores de activación, donde se solicita a los usuarios que inicien sesión usando sus credenciales de PASSPORT™ (etapa 152). Si el usuario no tiene una cuenta PASSPORT™, se le proporcionará un enlace para inscribirse para una (etapa 154). Se prefiere que el URL al servidor de activación esté preprogramado en un control 84 ACTIVEX de activación usando una conexión de SSL de manera que el cliente pueda garantizar que los servidores son verdaderamente los servidores de activación.

Una vez que el usuario está autenticado con PASSPORT™ (etapa 156), se solicita una API de PASSPORT™ para el alias del usuario y dirección de correo electrónico (etapa 158). Posteriormente, en las etapas 160-162, los servidores de activación solicitarán que el cliente (mediante el control ACTIVEX) cargue un ID de hardware único (que, como se ha indicado anteriormente, puede obtenerse desde componentes de hardware en el dispositivo informático del usuario que sustancialmente identifican de manera inequívoca el dispositivo informático del usuario). A continuación se determina si esta es una primera activación para el lector 92 (etapa 164). (En algunas circunstancias, los lectores pueden activarse más de una vez con diferentes ID de PASSPORT; si el lector 92 se ha activado con otro ID de PASSPORT, a continuación se presenta una advertencia, como se representa en la etapa 166).

Si se determina que esta es una nueva activación en la etapa 164, a continuación se determina si el usuario ha activado más de cinco lectores en los últimos 90 días. Si es así, a continuación se presenta un mensaje de error en la etapa 172 que incluye un número de teléfono de soporte, y el procedimiento termina en la etapa 198. Como se ha indicado anteriormente, la limitación de activar no más de cinco lectores en los últimos 90 días es simplemente ejemplar. Limitar la activación de los lectores por tiempo y número ayuda a evitar la amplia divulgación de un título de libro electrónico de nivel 5 para verse en miles (o millones) de lectores a lo largo de todo el mundo. Sin embargo, la limitación de “cinco lectores en noventa días” en el ejemplo de la Figura 5 es simplemente ejemplar, ya que pueden imponerse otras limitaciones en la activación sin alejarse del espíritu y alcance de la invención. Por ejemplo, la limitación de activación representada en la Figura 5 podría extenderse permitiendo activaciones adicionales una vez que transcurre un periodo de tiempo predeterminado, por ejemplo, una activación adicional después de que transcurre un periodo de 90 días posterior hasta un límite de 10 activaciones totales.

Si el usuario no ha activado más de cinco lectores en los primeros 90 días (o no se excluye de otra manera de activar el lector 92), se presenta una página de activación (etapa 170) para que el usuario la rellene. Si el usuario transmite el formulario en un formato incompleto (detectado en la etapa 174), la página puede volverse a presentar hasta que el usuario complete el formulario. A continuación en la etapa 176, se determina si la activación actual es una recuperación (es decir, un intento para “reactivar” un lector que se ha activado previamente pero que se vuelve no usable o desactivado por alguna razón). Si la presente activación no es una recuperación, entonces se crea un nuevo registro para el usuario y el lector y se incrementa el número de lectores asociados con el usuario (etapa 180). Un par de claves de repositorio seguro pre-generadas se recuperan desde una base de datos (etapa 182) y se generan también certificados de activación (etapa 184). (Como se ha analizado anteriormente, el certificado de activación puede incluir un par de claves pública/privada cuya clave privada se ha encriptado con la clave pública del par de claves del repositorio seguro). Las claves de activación, ID de usuario, e ID de máquina se hacen persistir en una base de datos (no mostrada) en la etapa 186. Preferentemente, las claves del repositorio seguro no se hacen persistir, y cualquier nuevo repositorio seguro que necesitara crearse y entregarse en el futuro tendría un nuevo par de claves (y el certificado de activación entregado con el que el nuevo repositorio seguro puede contener el par de

claves de activación que se han hecho persistir, pero con la clave privada encriptada a la (nueva) clave pública del (nuevo) repositorio seguro).

Si, en la etapa 176, se determina que esta activación es una recuperación, entonces se genera un certificado de activación (etapa 178) usando el par de claves pública/privada almacenadas desde una activación anterior (recuperándose el par de claves pública/privada desde la base de datos que se hizo persistir en la etapa 186), y el procesamiento continúa en la etapa 188.

En la etapa 188, el servidor o servidores de activación generan un ejecutable 82 de repositorio seguro. Preferentemente, el ejecutable 82 de repositorio seguro está firmado digitalmente, y basándose en y/o unido a un ID de máquina. El servidor o servidores de activación generan también un certificado de activación, que está preferentemente vinculado a la persona del usuario a través de su ID de PASSPORT™). El ejecutable 82 de repositorio seguro y el certificado de activación se descargan a continuación al cliente (etapas 188 y 190). El certificado de activación se encripta durante la descarga (por ejemplo, para proteger cualquier información contenida en el certificado que relaciona a la persona a la que está vinculado). El certificado de activación se carga más tarde a un servidor de “descarga” o “ejecución” durante el procedimiento de adquisición del libro electrónico descrito a continuación en relación con la Figura 6 (es decir, como parte del procedimiento para obtener un título de nivel 5). El ID de PASSPORT™ del usuario se encripta y marca en el registro del PC como parte de esta descarga (cuando se instala el lector 92 en un dispositivo informático que tiene un registro), para carga durante transacciones comerciales. El ID de PASSPORT™ se almacena por separado del certificado de activación (incluso aunque pueda incluirse en el certificado de activación) de modo que el ID de PASSPORT almacenado pueda compararse con el ID de PASSPORT en el certificado de activación durante la adquisición de un título de nivel 5, ayudando de esta manera a evitar el robo de contenido.

En la etapa 192 se determina si la descarga del repositorio 82 seguro y el certificado de activación ha sido satisfactoria. Si no, se registra un evento y se intenta de nuevo la descarga (etapas 194 y 192). Si la descarga fue satisfactoria, entonces en la etapa 196, puede proporcionarse al usuario con una página que “le felicita” al activar el lector 92 y le informa que el procedimiento de activación está completo. En un ejemplo, la página puede incluir enlaces donde el usuario puede obtener libros electrónicos “promocionales” o “gratis”. Este enlace cambiará dependiendo de la promoción (es decir, el servidor puede descargar una página diferente con diferentes enlaces si la “promoción” cambia). Este enlace puede aprovechar también un procedimiento expuesto mediante el control 84 ACTIVEX de activación para devolver al usuario a la página de biblioteca en el lector. El procedimiento a continuación termina en la etapa 198.

Flujo de procedimiento de comercio electrónico

Haciendo referencia ahora a la Figura 6, se describe una vista general del procedimiento básico por el que se obtienen y entregan títulos de libros electrónicos en línea. Se observa que el lector de la presente invención está adaptado para interactuar y operar en un entorno de servidor. Un servidor ejemplar de este tipo se describe en el Expediente del Mandatario N.º MSFT-0124, presentado de manera concurrente con el presente, que se incorpora expresamente por referencia en el presente documento en su totalidad.

Al usar un explorador o la característica de “biblioteca integrada” del lector 92, el usuario visita un sitio de venta minorista y elige el libro o libros de una manera implementada por el vendedor minorista (etapa 200). Por ejemplo, el sito puede proporcionar una página web que visualiza (como enlaces) diversos libros que el usuario puede desear comprar. El usuario a continuación paga los títulos (etapa 202), tal como enviando un número de tarjeta de crédito (o haciendo referencia a un número de tarjeta de crédito almacenado si el usuario tiene una cuenta con el sitio; en un uso, el ID de PASSPORT del usuario puede hacer referencia a un número o cuenta de este tipo). La transacción concluye en la etapa 204 con una página de recibo. La página de recibo puede contener información “que confirma” el pedido o agradece al usuario por su pedido, y contiene también enlaces (solicitudes POST de HTTP) para descargar cada título comprado. Para títulos completamente individualizados (nivel 5), un guion del lado de cliente rellena el cuerpo del POST con el certificado de activación, mediante el objeto 86 de comercio web. (Por ejemplo, el objeto 86 de comercio web se usa para recuperar el certificado de activación para provisión al sitio del vendedor minorista). En un ejemplo, el certificado de activación puede proporcionarse al sitio web del vendedor minorista, que a continuación crea una solicitud de HTTP (es decir, una solicitud POST) que incluye un objeto binario grande encriptado (es decir, en el cuerpo del POST). La solicitud de HTTP (que incluye el objeto binario grande encriptado) a continuación se presenta como un enlace en el sitio del cliente, donde el cliente hace clic en el enlace para descargar el título comprado (como se describe a continuación). En este escenario de ejemplo, la solicitud de HTTP y el objeto binario grande encriptado (que se generan por el vendedor minorista, que, preferentemente, está en privado con el sitio de ejecución) contiene información que identifica el libro electrónico particular a proporcionarse al comprador, así como información que demuestra al sitio de ejecución que el objeto binario grande encriptado se generó por un vendedor minorista para el que el sitio de ejecución ha acordado satisfacer pedidos de libros electrónicos. Adicionalmente, en el caso de la compra de títulos de nivel 5, el software del lado de cliente añade el certificado de activación al cuerpo del POST para permitir que se encripte la clave simétrica del libro electrónico para uso con lectores activados para la persona del usuario.

Tras hacer clic en cualquiera de los enlaces en la etapa 206, el explorador inicia una descarga desde un servidor de

descarga o “ejecución” especificado en la página de recibo. Para copias selladas individualmente (“inscritas”), el servidor de descarga añade el nombre del consumidor (u otra información de identificación según se determina mediante el sitio de venta minorista, tal como el número de tarjeta de crédito del usuario, un ID de transacción, etc.) a los metadatos de título y vuelve a sellar la clave simétrica usando el nuevo troceo criptográfico resultante de los nuevos metadatos, que ahora incluye tal información de identificación. (La información particular a incluirse se determina mediante el vendedor minorista y se proporciona como parte del objeto binario grande encriptado en el cuerpo del POST). Para copias completamente individualizadas (nivel 5) se genera y embebe una licencia en el fichero LIT, además de crearse el exlibris. La licencia contiene la clave simétrica que encriptó el fichero LIT “sellado” con la clave pública en el certificado de activación. Cuando la descarga está completa (etapa 208), el servidor de descarga registra la transacción y, en el cliente, el lector 92 puede lanzarse automáticamente (etapa 210). El título puede, en este momento, moverse en el almacenamiento local/almacenamiento LIT 98, u otra carpeta o directorio designado para el almacenamiento de títulos de libros electrónicos. Tras el lanzamiento del lector 92, el libro electrónico puede abrirse a su página 100 de cubierta.

De acuerdo con la presente invención, desde una perspectiva del usuario final, puede no haber diferencia perceptible entre un título protegido de nivel 3 y de nivel 5. Ambos incluyen un exlibris (por ejemplo, inclusión del nombre del usuario en la página 100 de cubierta). Los usuarios pueden únicamente advertir la diferencia si intentan mover un libro electrónico de nivel 5 a una instalación donde el lector 92 no se ha activado para la persona que compró el libro electrónico. En este caso, un título de nivel 5 no se abrirá en un lector 92 de este tipo, mientras que un título de nivel 3 se abrirá.

Escenarios de uso de cliente de sistema de DRM

La arquitectura de sistema de DRM se acciona por varios escenarios que los consumidores de libros electrónicos esperan encontrar. Los escenarios ejemplares se explican a continuación. Tales escenarios incluyen comprar un libro por impulso, leer un libro en múltiples lectores 92, activar un lector 92, y recuperar un título perdido o dañado. Los escenarios tienen variaciones de acuerdo con el nivel de protección de copia elegido por el proveedor de la publicación. Las variaciones impactan en el usuario puesto que determinan en algunos casos lo que el usuario debe hacer para obtener y abrir un título en uno o más lectores 92.

Comprar un libro electrónico por impulso y leer

Cuando un consumidor explora un sitio web del vendedor minorista usando un explorador web o una característica de “librería” dentro de la aplicación 92 del lector, él o ella selecciona libros a comprar (por ejemplo, crea un “carrito de la compra”), y continúa para pagar de acuerdo con las reglas y/o procedimientos del sitio de venta minorista. Dependiendo del nivel de protección asociado con los títulos seleccionados (que puede determinarse, por ejemplo, mediante el sitio de venta minorista, o el propietario de contenido en cuyo nombre distribuye el sitio de venta minorista el libro electrónico), el sitio de venta minorista puede solicitar información que identifica de manera inequívoca al consumidor. (Por ejemplo, si el título está protegido en nivel 3, el vendedor minorista obtiene el nombre del usuario desde una fuente (preferentemente) confiable para inclusión en los metadatos, de modo que un usuario no pudiera comprar un título bajo un falso nombre y escapar de la detección si el título se distribuyera ilícitamente. En este escenario, otra información desde la que puede trazarse al usuario, tal como el número de la tarjeta de crédito del usuario, un ID de transacción, etc., podría usarse para servir para el mismo fin). Si el título está protegido en nivel 5, el sitio de venta minorista necesitará también el certificado de activación (obtenido preferentemente por el uso del objeto 86 de comercio web y su guion encapsulador asociado) para encriptar apropiadamente la clave de contenido. Si el cliente/explorador no puede proporcionar la información requerida para completar la transacción, el sitio de venta minorista puede a continuación proporcionar al cliente con las etapas que se requieren (por ejemplo, en forma de una página web que explica las etapas y cómo pueden conseguirse y/o proporciona hiperenlaces a seguirse). Tras finalizar la transacción, se prefiere que el consumidor reciba un recibo para confirmar la transacción (es decir, una página de confirmación de pedido) o reciba errores de información que informen problemas con el procesamiento de su transacción de acuerdo con las reglas y políticas del sitio de venta minorista. A continuación, el comprador sigue instrucciones de descarga embebidas en el recibo para los libros que ha comprado, de acuerdo con las reglas y políticas expuestas por el sitio de venta minorista. (Por ejemplo, el recibo puede contener un hiperenlace para hacerse clic por el usuario para empezar la descarga de un libro electrónico). Después de que se ha descargado el libro electrónico, puede abrirse para lectura mediante el lector 92.

Leer un libro en múltiples lectores

Los consumidores esperaran poder leer títulos en más de una plataforma de lectura, por ejemplo, un PC de sobremesa, portátil, ordenador de bolsillo o un dispositivo de libro electrónico. El sistema de DRM de la presente invención contempla tal uso. Como parte del sistema de DRM, editores, y distribuidores y comerciantes pueden ser poseedores de claves simétricas que se usan para encriptar títulos de libros electrónicos. Preferentemente, se usa una clave por título o SKU/ISBN/EAN. La clave simétrica se requiere para abrir el título y está embebida en el flujo de licencia/DRM durante la compra. El procedimiento para encriptar y embeber más tarde la clave simétrica se denominará en el presente documento como “sellar”. Se observa que la clave simétrica puede encriptarse usando una clave pública asociada con el par de claves del certificado de activación del consumidor, o, en el caso de copias selladas de origen e individualmente, pueden encriptarse con un troceo criptográfico de los metadatos.

Para leer el título encriptado en múltiples lectores 92, cada instancia del lector 92 necesita poder acceder a la clave 14A simétrica embebida en el flujo de licencia/DRM del título. En el caso de títulos protegidos que no están completamente individualizados para una persona (por ejemplo, títulos en niveles 2, 3 o 4), acceder a la clave 14A simétrica se consigue usando (por ejemplo, troceando) los metadatos del título a sin sellar, y posiblemente desencriptando, la clave 14A simétrica, que se hace preferentemente mediante el gestor 80 de DRM. En este escenario, el comerciante/distribuidor del título encripta la clave 14A simétrica con un troceo criptográfico, que está generado por programación desde un troceo de los metadatos del título (que pueden incluir el nombre del propietario legítimo, por ejemplo, en el caso de títulos de nivel 3). El lector 92 y/o gestor de DRM 80 a continuación usa el mismo algoritmo de troceo para desellar la clave simétrica. Los usuarios que manipulen los contenidos de los metadatos del título ya no podrán leer el título del libro electrónico, puesto que el software de lector no podrá desencriptar/desellar la clave 14A simétrica, puesto que los nuevos metadatos darían como resultado un troceo diferente.

En el caso de títulos completamente individualizados (nivel 5), la clave 14A simétrica está encriptada con la clave pública del certificado de activación del usuario e insertada en la licencia, donde la licencia se inserta en el almacenamiento 14 de DRM en el flujo 14A (véase la Figura 4) antes de la descarga. Como se ha analizado anteriormente, cada lector 92 activado para una persona particular tiene un certificado de activación que contiene el par de claves pública/privada asociado con la persona. Por lo tanto, un título puede leerse en cualquier lector 92 que se haya activado para una persona particular. Como se ha analizado anteriormente, el certificado de activación se obtiene durante el procedimiento de activación. La “licencia” anteriormente mencionada, como se analiza adicionalmente a continuación, es una construcción que define los derechos que el consumidor puede ejercer tras la compra del contenido y, cuando está presente, contiene también la clave de contenido (es decir, la clave simétrica).

La arquitectura 90’ de cliente desencripta la clave simétrica encriptada contenida en la licencia de un título de nivel 5 aplicando la clave privada desde el certificado de activación, cuando la clave privada del certificado de activación está almacenada en forma encriptada y se obtiene usando el repositorio 82 seguro para aplicar su clave pública a la clave privada encriptada, como se ha analizado anteriormente. Más allá de asegurar que un lector 92 ha sido activado usando los credenciales (es decir, persona) para la que se preparó un título de nivel 5, no se requiere ninguna otra acción para permitir a un usuario leer un título en múltiples lectores 92. Además, incluso en el caso de títulos de nivel 5, el acto de asegurar que el lector está activado para la persona correcta tiene lugar implícitamente. - es decir, si el lector 92 no se ha activado para la persona con la que está asociado un título de nivel 5, a continuación el lector 92 no tendrá acceso al certificado de activación (y a su clave privada) que permite al lector acceder a la clave 14A simétrica necesaria para desencriptar el flujo 16 de contenido. Todos los títulos de nivel 5 comprados para un lector 92 tienen sus claves de contenido encriptadas para la clave pública incluida en el certificado de activación asociado con el lector/persona. Cuando el usuario instala o compra otro lector 92, el usuario únicamente necesita activar el nuevo lector con la misma persona para recibir el mismo certificado de activación (o, con más precisión, un certificado de activación equivalente con el mismo par de claves pública/privada, cuya clave privada, como se ha analizado anteriormente, está encriptada con la clave pública del repositorio seguro residente en el nuevo dispositivo/instalación de lectura).

Otra alternativa más para obtener la clave 14A simétrica existe a partir de una OpenCard. Cada OpenCard contiene una clave o par de claves a las que se sellan los títulos. Cuando el usuario desea leer los mismos títulos en un lector 92 diferente, el lector 92 debe instalarse en un dispositivo que tiene una ranura de OpenCard. Por consiguiente, cuando el usuario inserta la OpenCard en el dispositivo, los títulos están automáticamente disponibles para lectura. Por lo tanto, no se requieren etapas especiales cuando los usuarios desean leer títulos basados en OpenCard en múltiples lectores 92, puesto que, de hecho, el título está unido a la tarjeta en lugar de a un certificado de activación y/o persona particulares.

Mejorar o sustituir el lector

Si un usuario pierde, sustituye o mejora su lector, es importante que el usuario pueda leer títulos comprados previamente (por ejemplo, títulos de nivel 5) en el nuevo lector. De acuerdo con un aspecto de la invención, habilitar a los usuarios leer contenido previamente comprado en los nuevos lectores 92 se realiza usando los mismos mecanismos que para permitirles leer en múltiples lectores 92: el nuevo lector 92 obtiene el certificado de activación requerido (es decir, un certificado de activación con el par de claves contenido en los certificados de activación anteriores emitidos para la persona del usuario).

Hacer cumplir un límite en el número de activaciones de los lectores 92 de la manera anteriormente descrita simplifica el procedimiento de mejora/sustitución. Siempre que el usuario no supere el límite aplicable en activaciones, él puede activar un lector 92 nuevo/mejorado/de sustitución simplemente como si él estuviera activando otro de varios lectores de propiedad de ese usuario. Un usuario puede “cancelar” una activación de un lector antiguo borrando el certificado de activación, pero hacer esto no aumenta necesariamente el número de activaciones disponibles para una persona particular, puesto que la autoridad de activación (por ejemplo, los servidores de activación que los usuarios entran en contacto para obtener certificados de activación y los repositorios 82 seguros), no tienen necesariamente ninguna manera para verificar que el certificado de activación se ha borrado, o no se ha respaldado de una manera recuperable. Por lo tanto, en una realización de la invención, borrar el certificado de activación no “resetea” la limitación del entorno de nuevas activaciones para una persona

particular.

Recuperar un título perdido o dañado

Un usuario puede respaldar títulos, por ejemplo, copiando el fichero 10 de libro electrónico a un disco 29 magnético extraíble, disco 31 óptico, o una tarjeta de memoria no volátil extraíble. Si los títulos se perdieran o dañaran en el almacenamiento principal de un dispositivo de lectura particular, los títulos pueden restaurarse desde almacenamiento de respaldo. Sin embargo, en el caso donde los títulos, por alguna razón, no se respaldaran, puede ser posible recuperar cualquier título perdido o dañado desde el vendedor minorista. Por ejemplo, el usuario puede mantener la página de recibo desde una compra de título (es decir, la página que contiene los enlaces de descarga), y simplemente "volver a visitar" el enlace para conectar a un servidor de descarga para obtener una nueva copia del fichero 10 de libro electrónico ("LIT") que incorpora el título. Los usuarios pueden mantener sus recibos localmente o como alternativa, el almacenamiento de venta minorista puede elegir ofrecer a los clientes el servicio de almacenar sus recibos en el servidor del vendedor minorista.

En una realización preferida de la invención, sin embargo, los recibos tienen una hora/fecha de expiración (por ejemplo, el objeto binario grande encriptado asociado con el enlace que se ha hecho clic para entrar en contacto con el servidor de descarga puede tener una hora/fecha de expiración incorporada con él), de manera que haciendo clic en un enlace de descarga más de una cantidad de tiempo predeterminada después de que se emitió (por ejemplo, una hora) provocará que el servidor de descarga rechace descargar el fichero. En este caso, el vendedor minorista puede tener un registro de la compra y puede proporcionar una nueva copia del recibo/enlace de descarga. Para recuperar un título de libro electrónico perdido o dañado, el usuario tendrá que entrar en contacto con el comerciante desde el que se compró el título de libro electrónico. Después de que el usuario se ha identificado, el sitio del comerciante presentará al usuario una lista de recibos desde la que el usuario elegirá el apropiado. El usuario puede a continuación localizar el título que desea recuperar, y hacer clic en el enlace proporcionado para descarga. Excluyendo cualquier política restrictiva del sitio del comerciante, el usuario debería poder volver a descargar el título de libro electrónico que perdió. Generalmente no es necesario que el comerciante restringa la re-descarga de títulos, puesto que el usuario siempre es libre de copiar el título de máquina a máquina (sometido, por supuesto, a la condición de que los títulos de nivel 5 no funcionan en lectores activados para una persona distinta de la persona que compró el título), y por lo tanto restringir la re-descarga de títulos no proporciona protección de copia adicional. Debería observarse, sin embargo, que la decisión de proporcionar privilegios de "re-descarga" gratis es a discreción del comerciante, puesto que el comerciante puede ver la re-descarga como un servicio por el que el comerciante desee cobrar una tarifa.

Soportar múltiples lectores activados en el mismo PC

Se prefiere que el lector para PC portátiles y de sobremesa esté diseñado para soportar múltiples usuarios que compartan el mismo ordenador. Siempre que los usuarios tengan diferentes cuentas locales en el PC que comparten, el lector puede almacenar todos los datos específicos del usuario en el espacio de datos de usuario apropiado, separado de sus respectivos perfiles y valores de registro del "usuario actual". Por ejemplo, los ficheros 10 de libro electrónico pueden almacenarse, para cada usuario, en un directorio contenido lógicamente en el directorio de nivel superior para ese perfil de usuario. En el caso del procedimiento de activación, el procedimiento puede asegurar que el lector 92 que se está activando y que los componentes que se están descargando (por ejemplo, el repositorio 82 seguro y el certificado de activación) estén vinculados al usuario actual (por ejemplo, el usuario que ha iniciado sesión actualmente en una estación de trabajo que ejecuta el sistema operativo MICROSOFT WINDOWS NT).

Adicionalmente, una vez que se ha activado el lector, puede presentar el nombre PASSPORT™ para el usuario que lo activó, por ejemplo en una pantalla de bienvenida y una página de ajustes rápidos. En la página de ajustes rápidos, el nombre de PASSPORT™ para el usuario que ha activado por última vez el lector se mostrará inmediatamente por encima del enlace de activación. Esto permite el manejo apropiado mediante el objeto 86 de comercio web del lado de cliente del certificado de activación y carga de ID de PASSPORT™ encriptado, durante el procedimiento de hacer compras de títulos completamente individualizados (protegidos de nivel 5).

El procedimiento mediante el cual múltiples usuarios pueden activar el mismo lector 92 en un sistema compartido ejemplar es como sigue. El lector comprobará si se ha activado durante el arranque. Esta comprobación se realiza comprobado una clave de registro de activación completa (ActivationComplete), bajo HKEY_CURRENT_USER\Software\Microsoft\libro_electrónico\ (HKEY_CURRENT_USER\Software\Microsoft\eBook\). Puesto que esta clave de registro se escribe en la rama HKCU, asegura que será específica de usuario y estará vinculada al nombre de usuario que ha iniciado sesión actualmente en el ordenador. Si esta clave de registro no se encuentra o no está establecida a 1 (es decir, ha tenido lugar una activación satisfactoria) el usuario sigue las etapas para activar el lector, como se ha analizado anteriormente. Después de que la descarga está completa, el control 84 ACTIVEX de activación solicita al sistema operativo el nombre de usuario del usuario que ha iniciado sesión actualmente en el PC. Si no se devuelve nombre de usuario, se supondrá "Usuario por defecto" (DefaultUser) como el nombre de usuario.

El control 84 ACTIVEX a continuación solicita al registro para encontrar dónde se instaló el lector. A continuación crea un directorio bajo el directorio de instalación de MS Reader que se nombrará: .\<nombre_de_usuario>\repositorio_seguro (.\<username>\SecureRepository) (<nombre de usuario> según se determina por la consulta del sistema operativo). Una vez que se crea el directorio, el control 84 ACTIVEX rellena la clave HKCU\..\libro_electrónico\repositorio_seguro (HKCU\..\eBook\SecureRepository), con la ruta completa a ese directorio. En ese directorio, el control 84 ACTIVEX instala el repositorio 82 seguro y el certificado de activación. A continuación ejecuta el repositorio 82 seguro con el parámetro “-instalar” (-install) para auto-registro del repositorio 82 seguro. Suponiendo que todas las etapas anteriores tuvieron éxito, el control 84 ACTIVEX marca la clave de registro de activación completa.

Formato de licencia

A continuación se encuentra una licencia ejemplar, que se usa para cada descarga de títulos completamente individualizados. La licencia es una construcción que define los derechos que el usuario puede ejercer tras la compra del título, además de definir los requisitos para desellar la clave simétrica para ejercer estos derechos. Ejemplos de “derechos” que podrían representarse en la licencia son presentar el contenido (por ejemplo, en el ejemplo de contenido de texto, leerlo en el monitor de un PC), imprimir el contenido, o copiar y pegar porciones del contenido. Se observa que el formato de licencia ejemplar no se pretende para limitar el alcance de la presente invención ya que son posibles otros formatos de licencia que tienen mayor o menor información.

Se prefiere que el lenguaje elegido para representar una licencia sea XML, y el formato de la licencia esté basado en la especificación del Lenguaje de Marcado de Derechos Extendido (XrML). Este es un lenguaje de marcado bien conocido para describir derechos de uso de una manera flexible. XrML también proporciona gran interoperabilidad y permitirá que se aproveche cualquier inversión de tecnología realizada en componentes que generan y gestionan estas licencias a largo plazo. En una realización preferida, únicamente aquello expresado en la licencia se concede a la licencia - es decir, si un derecho no está expresamente concedido, se deniega. Sin embargo, se apreciará por los expertos en la materia que son posibles otras disposiciones, tal como cuando se supone un conjunto de derechos por defecto a menos que se deniegue o modifique expresamente por la licencia.

Las etiquetas de nivel superior en un formato contraído son como sigue:

```
<?xml version="1.0" ?>
        <!DOCTYPE XrML SYSTEM "xrml.dtd">
      - <XrML>
        - <BODY type="LICENSE" version="2.0">
            <ISSUED>2000-01-27T15:30</ISSUED>
          + <DESCRIPTOR>
          - <!-- ============================================
            -->
          - <!-- Libro con licencia
            -->
          - <!-- ============================================
            -->
          + <WORK>
            ==========================================
              ======
              Componentes del libro
              Un capítulo, y una imagen con valor de resumen
            ==========================================
              ======

            ==========================================
              ======
                    Derechos de uso del libro
            ==========================================
              ======

        - <!-- ============================================
          -->
```

```
- <!-- Licenciatario del libro
  -->
- <!-- ═══════════════════════════════════════
  -->
+ <LICENSOR>
- <!-- ═══════════════════════════════════════
  -->
- <!-- Licencias del libro
  -->
- <!-- ═══════════════════════════════════════
  -->
+ <LICENSEDPRINCIPALS>
</BODY>
- <!-- ═══════════════════════════════════════ --
  >
- <!-- Firma del cuerpo de la licencia
  -->
- <!-- ═══════════════════════════════════════ --
  >
+ <SIGNATURE>
</XrML>
```

La primera línea de la estructura XrML anterior define la versión del lenguaje de XML usado para crear la licencia XrML. La segunda línea especifica el nombre del fichero DTD usado para analizar el fichero XML. La etiqueta BODY (CUERPO) proporciona el tipo de licencia, la versión de la especificación de XrML usada cuando se generó la licencia, y la fecha cuando se emitió. Es también la meta-etiqueta para toda la licencia, que tiene las siguientes subsecciones: WORK (TRABAJO), LICENSOR (LICENCIATARIO), LICENSEDPRINCIPALS (REPRESENTADOS CON LICENCIA), y SIGNATURE (FIRMA). WORK contiene toda la información semántica acerca de la licencia, incluyendo los derechos (RIGHTS) de uso. Los contenidos de este campo (incluyendo las etiquetas) constituyen los datos que se trocearon y firmaron. LICENSOR contiene información que pertenece a la entidad que emitió la licencia, normalmente un vendedor minorista. LICENSEDPRINCIPALS contiene una serie de representados que deben autenticarse cuando se ejercen los derechos de uso especificados en una licencia. SIGNATURE contiene el troceo/resumen del LICENSEBODY (CUERPO DE LICENCIA) así como información acerca de cómo se creó el troceo, incluyendo el algoritmo usado. Incluye también el DIGEST (RESUMEN) codificado de acuerdo con el algoritmo nombrado por el licenciatario cuando se emite la licencia. Las etiquetas DIGEST y SIGNATURE proporcionan la información de autenticación usada para validar toda la licencia de una manera con la que no pueda manipularse.

Estructura de la etiqueta BODY

La etiqueta principal de una construcción de licencia de XrML es la etiqueta BODY, que contiene las siguientes etiquetas:

```
- <BODY type="LICENSE" version="2.0">
    <ISSUED>2000-01-27T15:30</ISSUED>
  - <DESCRIPTOR>
    - <OBJECT type="self-proving-EUL">
        <ID type="MS-GUID">7BD394EA-C841-434d-
          A33F-5456D5E2AAAE</ID>
      </OBJECT>
    </DESCRIPTOR>
  - <!-- ========================================== -->
  - <!-- Libro con licencia                          --
    >
  - <!-- ========================================== -->
  - <WORK>
    - <OBJECT type="BOOK-LIT-FORMAT">
        <ID type="ISBN">8374-39384-38472</ID>
        <NAME>A book of James</NAME>
      </OBJECT>
      <CREATOR type="author">James the
        first</CREATOR>
      <CREATOR type="author">James the
        second</CREATOR>
    - <OWNER>
      - <OBJECT type="Person">
          <ID type="US-SSN">103-74-8843</ID>
          <NAME>Mike the man</NAME>
```

```
        <ADDRESS
          type="email">mike@man.com</ADDRE
          SS>
      </OBJECT>
    - <PUBLICKEY>
        <ALGORITHM>RSA-512</ALGORITHM>
      - <PARAMETER name="public exponent">
          <VALUE
            encoding="integer32">65537</VAL
            UE>
        </PARAMETER>
      - <PARAMETER name="modulus">
          <VALUE encoding="base64"
            size="512">u+aEb/WqgyO+aDjgYL
            xwrktqFDR4HZeIeR1g+G5vmKNZRt
            9FH4ouePWz/AJYnn2NdxoJ6mcIIAQ
            Ve6Droj2fxA==</VALUE>
        </PARAMETER>
      </PUBLICKEY>
    </OWNER>
  - <!-- ============================================-->
  - <!-- Componentes del libro
      -->
  - <!-- Un capítulo, y una imagen con valor de resumen -->
  - <!-- ============================================-->
  - <PARTS>
    - <WORK>
      - <OBJECT type="Chapter">
          <ID type="relative">0</ID>
          <NAME>Chapter 1</NAME>
        </OBJECT>
      </WORK>
    - <WORK>
      - <OBJECT type="Image">
          <ID type="relative">1</ID>
```

```
            <NAME>Image 1: Photon Celebshots
              Dogs</NAME>
          </OBJECT>
        - <DIGEST sourcedata="LicensorMeta">
            <ALGORITHM>SHA1</ALGORITHM>
          - <PARAMETER name="codingtype">
              <VALUE
                encoding="string">surface-
                coding</VALUE>
            </PARAMETER>
            <VALUE encoding="base64"
              size="160">OtSrhD5GrzxMeFEm8q
              4pQICKWHI=</VALUE>
          </DIGEST>
        </WORK>
      </PARTS>
    - <!-- ============================================-->
    - <!-- Derechos de uso del libro                   --
      >
    - <!-- ============================================-->
    - <RIGHTSGROUP name="Main Rights">
        <DESCRIPTION>Some desc</DESCRIPTION>
      - <BUNDLE>
        - <TIME>
            <FROM time="2000-01-27T15:30" />
            <UNTIL time="2000-01-27T15:30" />
          </TIME>
        - <ACCESS>
          - <PRINCIPAL sequence="2">
            - <ENABLINGBITS type="sealed-
                des-key">
                <VALUE encoding="base64"
                  size="512">lnHtn/t2dp3u
                  +ZqLkbd7MK0K4xR4YdSX
                  aEvuk2Loh9ZRJEcPzCw+x
```

```
                M7zbPrJb6ESj70+B2fWTcx
                xDD+6WUB/Lw==</VALU
                E>
            </ENABLINGBITS>
        </PRINCIPAL>
    </ACCESS>
</BUNDLE>
- <RIGHTSLIST>
  - <VIEW>
    - <ACCESS>
      - <PRINCIPAL sequence="2">
        - <ENABLINGBITS
              type="sealed-des-key">
              <VALUE
                encoding="base64"
                size="512">lnHtn/t2d
                p3u+ZqLkbd7MK0K4x
                R4YdSXaEvuk2Loh9Z
                RJEcPzCw+xM7zbPrJb
                6ESj70+B2fWTcxxDD
                +6WUB/Lw==</VAL
                UE>
            </ENABLINGBITS>
        </PRINCIPAL>
        <PRINCIPAL sequence="3" />
    </ACCESS>
  - <ACCESS>
    - <PRINCIPAL type="licensor">
      - <ENABLINGBITS
            type="sealed-des-key">
            <VALUE
              encoding="base64"
              size="512">lnHtn/t2d
              p3u+ZqLkbd7MK0K4x
              R4YdSXaEvuk2Loh9Z
```

```
                RJEcPzCw+xM7zbPrJb
                6ESj70+B2fWTcxxDD
                +6WUB/Lw==</VAL
                UE>
            </ENABLINGBITS>
        </PRINCIPAL>
    </ACCESS>
</VIEW>
- <PRINT maxcount="5">
  - <FEE>
    - <MONETARY>
      - <PERUSE value="5.00">
            <CURRENCY iso-
              code="USD" />
        </PERUSE>
      - <ACCOUNT>
            <ACCOUNTFROM
              id="BA-0234-
              0928392" />
            <HOUSE id="XYZ"
              url="http://somehous
              e.com/payme.asp" />
        </ACCOUNT>
    </MONETARY>
  </FEE>
- <TRACK>
    <PROVIDERNAME>e-
      tracker</PROVIDERNAME>
    <PROVIDERID id="US1023"
      type="Tracker ID" />
  - <PARAMETER name="tracking
      address">
      <VALUE
        encoding="url">"http://so
```

```
                    metrackingservice/trackm
                    e.asp"></VALUE>
                </PARAMETER>
              - <PARAMETER name="tracking
                  support address">
                  <VALUE
                    encoding="url">"http://so
                    metrackingservice/support
                    me.asp"></VALUE>
                </PARAMETER>
              </TRACK>
            - <TERRITORY>
                <LOCATION country="us"
                  state="CA" city="El Segundo"
                  postalcode="90245" />
                <LOCATION country="jp" />
              </TERRITORY>
            </PRINT>
          </RIGHTSLIST>
        </RIGHTSGROUP>
      </WORK>
    - <!--=============================================-->
    - <!-- Licenciatario del libro                    -->
    - <!--=============================================-->
    - <LICENSOR>
      - <OBJECT type="Principal-Certificate">
          <ID type="MS-GUID">7BD394EA-C841-434d-
            A33F-5456D5E2AAAE</ID>
          <NAME>Barnes and Noble</NAME>
        </OBJECT>
      - <PUBLICKEY>
          <ALGORITHM>RSA-512</ALGORITHM>
        - <PARAMETER name="public exponent">
            <VALUE
              encoding="integer32">65537</VALUE>
```

```
        </PARAMETER>
      - <PARAMETER name="modulus">
          <VALUE encoding="base64"
            size="512">u+aEb/WqgyO+aDjgYLxwrk
            tqFDR4HZeIeR1g+G5vmKNZRt9FH4oueP
            Wz/AJYnn2NdxoJ6mcIIAQVe6Droj2fxA=
            =</VALUE>
        </PARAMETER>
      </PUBLICKEY>
    </LICENSOR>
- <!-- ============================================ -->
- <!-- Licencias del libro                          -->
- <!-- ============================================ -->
- <LICENSEDPRINCIPALS>
    - <PRINCIPAL>
      - <OBJECT type="program">
          <ID
            type="msprogid">XrML.interpreter</ID
            >
          <NAME>DRPL INTERPRETER</NAME>
        </OBJECT>
      - <AUTHENTICATOR type="drm-module-
          verifier">
          <ID type="microsoft-
            progid">ms.drm.authenticode</ID>
          <NAME>DRMAuthenticode</NAME>
        - <AUTHENTICATIONCLASS>
            <VERSIONSPAN min="2.0" max="3.4"
              />
            <VERSION>5.0</VERSION>

              <SECURITYLEVEL>5</SECURITYLE
              VEL>
          </AUTHENTICATIONCLASS>
```

```
- <VERIFICATIONDATA type="signature-
    key">
  - <PUBLICKEY>
      <ALGORITHM>RSA-
        512</ALGORITHM>
    - <PARAMETER name="public
        exponent">
        <VALUE
          encoding="integer32">65
          537</VALUE>
      </PARAMETER>
    - <PARAMETER name="modulus">
        <VALUE encoding="base64"
          size="512">u+aEb/Wqgy
          O+aDjgYLxwrktqFDR4HZe
          IeR1g+G5vmKNZRt9FH4o
          uePWz/AJYnn2NdxoJ6mcII
          AQVe6Droj2fxA==</VALU
          E>
      </PARAMETER>
    </PUBLICKEY>
  </VERIFICATIONDATA>
</AUTHENTICATOR>
</PRINCIPAL>
- <PRINCIPAL>
  - <OBJECT type="MS Ebook Device">
      <ID type="INTEL SN">Intel PII 92840-
        AA9-39849-00</ID>
      <NAME>Johns Computer</NAME>
    </OBJECT>
  - <AUTHENTICATOR type="drminternal-
      certverify-program">
      <ID type="microsoft-progid">2323-2324-
        abcd-93a1</ID>
    - <AUTHENTICATIONCLASS>
```

<VERSION>1.x-2.5</VERSION>
</AUTHENTICATIONCLASS>
- <VERIFICATIONDATA type="authenticode-named-root">
- <PUBLICKEY>
<ALGORITHM>RSA-512</ALGORITHM>
- <PARAMETER name="public exponent">
<VALUE encoding="integer32">65537</VALUE>
</PARAMETER>
- <PARAMETER name="modulus">
<VALUE encoding="base64" size="512">u+aEb/WqgyO+aDjgYLxwrktqFDR4HZeIeR1g+G5vmKNZRt9FH4ouePWz/AJYnn2NdxoJ6mcIIAQVe6Droj2fxA==</VALUE>
</PARAMETER>
</PUBLICKEY>
</VERIFICATIONDATA>
- <VERIFICATIONDATA>
- <PARAMETER name="bbid">
<VALUE encoding="string">xxzzy</VALUE>
</PARAMETER>
- <PUBLICKEY>
<ALGORITHM>RSA-512</ALGORITHM>
- <PARAMETER name="public exponent">

```
                <VALUE
                  encoding="integer32">3<
                  /VALUE>
              </PARAMETER>
            - <PARAMETER name="modulus">
                <VALUE encoding="base64"
                  size="90">33845URT2039
                  87==</VALUE>
              </PARAMETER>
            </PUBLICKEY>
          </VERIFICATIONDATA>
        </AUTHENTICATOR>
      </PRINCIPAL>
    - <PRINCIPAL>
      - <OBJECT type="application">
          <ID type="MS PROG-
            ID">43984938476jshd</ID>
          <NAME>MS Book Reader 2.0</NAME>
        </OBJECT>
      - <AUTHENTICATOR type="drminternal-digest-
          program">
          <ID type="microsoft-progid">2323-2324-
            abcd-93a1</ID>
        - <AUTHENTICATIONCLASS>
            <VERSION>1.x-2.5</VERSION>
          </AUTHENTICATIONCLASS>
        - <VERIFICATIONDATA type="authenticode-
            named-root">
          - <DIGEST>

              <ALGORITHM>MD5</ALGORIT
              HM>
            <VALUE encoding="base64"
              size="90">bXlwYXNzd29yZA=
              =</VALUE>
```

```
                    </DIGEST>
                  </VERIFICATIONDATA>
                </AUTHENTICATOR>
              </PRINCIPAL>
            </LICENSEDPRINCIPALS>
          </BODY>
```

Autenticidad de licencia

El Repositorio 82 seguro autentica una licencia mediante las etiquetas SIGNATURE y DIGEST. Esto es de manera que el software cliente puede validar que el contenido que se está representado proviene de una fuente confiable. Se proporciona un ejemplo más detallado de estas etiquetas a continuación:

```
- <!-- ═══════════════════════════════════════
        Firma del cuerpo de la licencia

     ═══════════════════════════════════════
     -->
- <SIGNATURE>
  - <DIGEST>
      <ALGORITHM>SHA1</ALGORITHM>
    - <PARAMETER name="codingtype">
        <VALUE encoding="string">surface-
          coding</VALUE>
      </PARAMETER>
      <VALUE encoding="base64"
        size="160">OtSrhD5GrzxMeFEm8q4pQICKW
        HI=</VALUE>
    </DIGEST>
    <VALUE encoding="base64"
      size="512">A7qsNTFT2roeL6eP+IDQFwjIz5XSFBV
      +NBF0eNa7de+1D6n+MPJa3J7ki8Dmwmuu/pBciQ
      nJ4xGaqRZ5AYoWRQ==</VALUE>
  </SIGNATURE>
```

Se observa que los anteriores ejemplos se han proporcionado simplemente para el fin de explicación y no se han de interpretar de ninguna manera como limitantes de la presente invención. Aunque la invención se ha descrito con referencia a las diversas realizaciones, se entiende que las palabras que se han usado en el presente documento son palabras de descripción e ilustración, en lugar de palabras de limitaciones. Además, aunque la invención se ha descrito en el presente documento con referencia a medios, materiales y realizaciones particulares, la invención no pretende estar limitada a los detalles particulares desvelados en el presente documento; en su lugar, la invención se

extiende a toda estructura, procedimiento y uso funcionalmente equivalente, tal como están dentro del alcance de las reivindicaciones adjuntas. Los expertos en la materia, que tienen el beneficio de las enseñanzas de esta memoria descriptiva, pueden efectuar numerosas modificaciones a la misma y pueden realizarse cambios sin alejarse del alcance de la invención en sus aspectos.

Lo siguiente es una lista de realizaciones no reivindicadas de la invención:

Realización 1. Un dispositivo informático adaptado para comunicar mediante una infraestructura de red, que comprende:

un dispositivo de almacenamiento a largo plazo;
una interfaz de usuario adaptada para interactuar con el dispositivo informático y para lanzar una aplicación de presentación; y
un módulo de gestión que recibe una comunicación desde la aplicación de presentación para acceder a una primera información almacenada en el dispositivo de almacenamiento a largo plazo, en el que la primera información está almacenada en un formato encriptado y en el que el módulo de gestión devuelve primeros datos que habilitan el uso de dicha primera información mediante dicha aplicación de presentación.

Realización 2. El dispositivo informático de la realización 1, en el que dichos primeros datos comprenden una clave para desencriptar dicha primera información.

Realización 3. El dispositivo informático de la realización 1, en el que dichos primeros datos incluyen dicha primera información en un formato desencriptado.

Realización 4. El dispositivo informático de la realización 1, en el que la segunda información que pertenece a un usuario o una transacción se devuelve mediante el módulo de gestión a la aplicación de presentación para uso en el dispositivo informático.

Realización 5. El dispositivo informático de la realización 4, en el que dicha segunda información se selecciona a partir del grupo que consiste en: un nombre, un número de tarjeta de crédito, y un número de recibo.

Realización 6. El dispositivo informático de la realización 1, en el que dicho módulo de gestión autentica dicha aplicación de presentación antes de devolver dichos primeros datos.

Realización 7. El dispositivo informático de la realización 1, en el que dicho módulo de gestión puede interconectarse con un repositorio seguro que puede recibirse mediante dicha infraestructura de red, en el que dicho repositorio seguro aplica una clave a los segundos datos.

Realizaciones 8. El dispositivo informático de la realización 1, en el que dichos segundos datos comprenden una clave que desencripta dicha primera información.

Realización 9. Un medio legible por ordenador que tiene instrucciones ejecutables por ordenador para realizar actos que comprenden:

autenticar software; y

proporcionar al menos un servicio criptográfico para dicho software;

en el que dichas instrucciones ejecutables por ordenador para realizar dicho al menos un servicio criptográfico pueden invocarse mediante una llamada desde dicho primer software.

Realización 10. El medio legible por ordenador de la realización 9, en el que dicho al menos un servicio criptográfico comprende usar una clave criptográfica para desencriptar datos.

Realización 11. El medio legible por ordenador de la realización 9, en el que dicho al menos un servicio criptográfico comprende desellar datos sellados.

Realización 12. El medio legible por ordenador de la realización 11, en el que dichos datos sellados comprenden una clave criptográfica.

Realización 13. El medio legible por ordenador de la realización 11, en el que dichos datos sellados comprenden información asociada con el usuario cuyo contenido tiene licencia.

Realización 14. El medio legible por ordenador de la realización 13, en el que dicha información se selecciona a partir del grupo que consiste en: un nombre, un número de tarjeta de crédito, y un número de recibo.

Realización 15. El medio legible por ordenador de la realización 9, en el que dicho acto para proporcionar al menos un servicio criptográfico comprende emitir una llamada a un repositorio seguro, en el que dicho repositorio seguro desencripta al menos algunos datos.

Realización 16. Un procedimiento de uso de primera información almacenada en un formato encriptado, comprendiendo dicho procedimiento los actos de:

emitir una primera solicitud para proporcionar primeros datos que habilitan el uso de dicha primera información; y

si dicha primera información está sellada con segunda información que pertenece a un usuario autorizado de dicha primera información, emitir una segunda solicitud para proporcionar segundos datos que incluyen dicha segunda información.

Realización 17. El procedimiento de la realización 16, en el que dicha segunda información se selecciona del grupo que consiste en: un nombre, un número de tarjeta de crédito y un número de recibo.

Realización 18. El procedimiento de la realización 16, en el que dichos primeros datos comprenden dicha primera información en un formato desencriptado.

Realización 19. El procedimiento de la realización 16, en el que dichos primeros datos comprenden una clave que desencripta dicha primera información.

Realización 20. El procedimiento de la realización 16, en el que dicha primera solicitud se emite a un objeto que satisface dichas solicitudes.

Realización 21. El procedimiento de la realización 20, en el que dicho objeto comprende un objeto COM.

REIVINDICACIONES

1. Un procedimiento de soporte de un sistema de distribución de contenido, comprendiendo dicho procedimiento los actos de:

proporcionar, a una primera entidad, una interfaz para solicitar al menos un servicio, siendo usable dicha interfaz mediante un lector (92) de contenido; y
proporcionar, a una segunda entidad, un conjunto de instrucciones ejecutables por ordenador que proporcionan uno o más servicios;

en el que dichas instrucciones ejecutables por ordenador pueden invocarse por medio de dicha interfaz, y en el que dicho uno o más servicios incluyen habilitar el uso de contenido digital almacenado en una forma encriptada en un dispositivo (90, 90') informático, y en el que dicho conjunto de instrucciones ejecutables por ordenador incluye instrucciones para:

activar el lector de contenido en el dispositivo informático, generando la activación un certificado que reside en el dispositivo informático y que contiene una clave privada de certificado, la clave privada de certificado encriptada mediante una clave pública de un repositorio (82) seguro en el dispositivo informático, descargando la activación también el repositorio seguro al dispositivo informático;
emitir una llamada al repositorio seguro descargado si dicho contenido digital tiene asociado con el mismo un primer nivel de protección, en el que el depositario seguro desencripta la clave privada de certificando usando una clave privada de repositorio seguro, en el que la clave privada de certificado se usa para desencriptar una clave simétrica que encripta el contenido digital, y en el cual el contenido digital se lee mediante el lector de contenido y se presenta a un usuario del dispositivo informático; y habilita el uso de dicho contenido digital en el dispositivo informático sin usar dicho repositorio seguro descargado si dicho contenido digital tiene asociado con el mismo un segundo nivel de protección diferente de dicho primer nivel de protección.

2. El procedimiento de la reivindicación 1, en el que dicha primera entidad comprende un desarrollador de dicho lector de contenido.

3. El procedimiento de la reivindicación 1, en el que dicha segunda identidad comprende un consumidor de dicho contenido digital.

4. El procedimiento de la reivindicación 1, en el que dicho conjunto de instrucciones ejecutables por ordenador comprenden un objeto COM.

5. El procedimiento de la reivindicación 1, en el que dicho uno o más servicios incluyen desencriptar dicho contenido digital para provisión a dicho lector de contenido.

6. El procedimiento de la reivindicación 1, en el que dicho uno o más servicios incluyen proporcionar a dicho lector de contenido una clave para desencriptar dicho contenido digital.

7. El procedimiento de la reivindicación 1, en el que dicho uno o más servicios incluyen proporcionar a dicho lector de contenido un nombre de un usuario autorizado de dicho contenido digital.

8. El procedimiento de la reivindicación 1, en el que dicho uno o más servicios incluyen desellar al menos alguno de dicho contenido digital.

9. El procedimiento de la reivindicación 1, en el que dicho uno o más servicios incluyen autenticar dicho lector de contenido.

10. El procedimiento de la reivindicación 1, en el que dicho acto de proporcionar a dicha primera entidad se realiza por dicha primera entidad.

11. Uno o más medios legibles por ordenador codificados con primeras instrucciones ejecutables por ordenador para realizar un procedimiento que comprende los actos de:

proporcionar, a una primera entidad, una interfaz para solicitar al menos un servicio, siendo usable dicha interfaz mediante un lector (92) de contenido; y
proporcionar, a una segunda entidad, un conjunto de segundas instrucciones ejecutables por ordenador que proporcionan uno o más servicios;

en el que dichas segundas instrucciones ejecutables por ordenador son invocadas por medio de dicha interfaz, y en el que dicho uno o más servicios incluyen habilitar el uso de contenido digital almacenado en una forma encriptada en un dispositivo (90, 90') informático, y en el que dicho conjunto de segundas instrucciones ejecutables por ordenador incluye instrucciones para:

activar el lector de contenido en el dispositivo informático, generando la activación un certificado que reside en el dispositivo informático y que contiene una clave privada de certificado, la clave privada de certificado encriptada

mediante una clave pública de un repositorio (82) seguro en el dispositivo informático, descargando la activación también el repositorio seguro al dispositivo informático;
emitir una llamada al repositorio seguro descargado si dicho contenido digital tiene asociado con el mismo un primer nivel de protección, en el que el depositario seguro desencripta la clave privada de certificando usando una clave privada de repositorio seguro, en el que la clave privada de certificado se usa para desencriptar una clave simétrica que encripta el contenido digital, y en el cual el contenido digital se lee mediante el lector de contenido y se presenta a un usuario del dispositivo informático; y habilita el uso de dicho contenido digital en el dispositivo informático sin usar dicho repositorio seguro descargado si dicho contenido digital tiene asociado con el mismo un segundo nivel de protección diferente de dicho primer nivel de protección.

12. El uno o más medios legibles por ordenador de la reivindicación 11, en el que dicha primera entidad comprende un desarrollador de dicho lector de contenido.

13. El uno o más medios legibles por ordenador de la reivindicación 11, en el que dicha segunda identidad comprende un consumidor de dicho contenido digital.

14. El uno o más medios legibles por ordenador de la reivindicación 11, en el que dicho segundo conjunto de instrucciones ejecutables por ordenador comprende un objeto COM.

15. El uno o más medios legibles por ordenador de la reivindicación 11, en el que dicho uno o más servicios incluyen desencriptar dicho contenido digital para provisión a dicho lector de contenido.

16. El uno o más medios legibles por ordenador de la reivindicación 11, en el que dicho uno o más servicios incluyen proporcionar a dicho lector de contenido una clave para desencriptar dicho contenido digital.

17. El uno o más medios legibles por ordenador de la reivindicación 11, en el que dicho uno o más servicios incluyen proporcionar a dicho lector de contenido un nombre de un usuario autorizado de dicho contenido digital.

18. El uno o más medios legibles por ordenador de la reivindicación 11, en el que dicho uno o más servicios incluyen desellar al menos alguno de dicho contenido digital.

19. El uno o más medios legibles por ordenador de la reivindicación 11, en el que dicho uno o más servicios incluyen autenticar dicho lector de contenido.

20. El uno o más medios legibles por ordenador de la reivindicación 11, en el que dicho acto de proporcionar a dicha primera entidad se realiza por dicha primera entidad.

21. Un sistema informático para soportar un sistema de distribución de contenido, comprendiendo el sistema:

medios para proporcionar, a una primera entidad, una interfaz para solicitar al menos un servicio, siendo usable dicha interfaz mediante dicho lector (92) de contenido; y
medios para proporcionar, a una segunda entidad, un conjunto de instrucciones ejecutables por ordenador que proporcionan uno o más servicios;

en el que dichas instrucciones ejecutables por ordenador pueden invocarse por medio de dicha interfaz, y en el que dicho uno o más servicios incluyen habilitar el uso de contenido digital almacenado en una forma encriptada en un dispositivo (90, 90') informático, y en el que dicho conjunto de instrucciones ejecutables por ordenador incluye instrucciones para:

activar el lector de contenido en el dispositivo informático, generando la activación un certificado que reside en el dispositivo informático y que contiene una clave privada de certificado, la clave privada de certificado encriptada mediante una clave pública de un repositorio (82) seguro en el dispositivo informático, descargando la activación también el repositorio seguro al dispositivo informático;
emitir una llamada al repositorio seguro descargado si dicho contenido digital tiene asociado con el mismo un primer nivel de protección, en el que el depositario seguro desencripta la clave privada de certificando usando una clave privada de repositorio seguro, en el que la clave privada de certificado se usa para desencriptar una clave simétrica que encripta el contenido digital, y en el cual el contenido digital se lee mediante el lector de contenido y se presenta a un usuario del dispositivo informático; y habilita el uso de dicho contenido digital en el dispositivo informático sin usar dicho repositorio seguro descargado si dicho contenido digital tiene asociado con el mismo un segundo nivel de protección diferente de dicho primer nivel de protección.

22. El sistema informático de la reivindicación 21, en el que dicha primera entidad comprende un desarrollador de dicho lector de contenido.

23. El sistema informático de la reivindicación 21, en el que dicha segunda identidad comprende un consumidor de dicho contenido digital.

24. El sistema informático de la reivindicación 21, en el que dicho conjunto de instrucciones ejecutables por ordenador comprende un objeto COM.

25. El sistema informático de la reivindicación 21, en el que dicho uno o más servicios incluyen desencriptar dicho contenido digital para provisión a dicho lector de contenido.

26. El sistema informático de la reivindicación 21, en el que dicho uno o más servicios incluyen proporcionar a dicho lector de contenido una clave para desencriptar dicho contenido digital.

27. El sistema informático de la reivindicación 21, en el que dicho uno o más servicios incluyen proporcionar a dicho lector de contenido un nombre de un usuario autorizado de dicho contenido digital.

28. El sistema informático de la reivindicación 21, en el que dicho uno o más servicios incluyen desellar al menos alguno de dicho contenido digital.

29. El sistema informático de la reivindicación 21, en el que dicho uno o más servicios incluyen autenticar dicho lector de contenido.

30. El sistema informático de la reivindicación 21, en el que dicho acto de proporcionar a dicha primera entidad se realiza por dicha primera entidad.

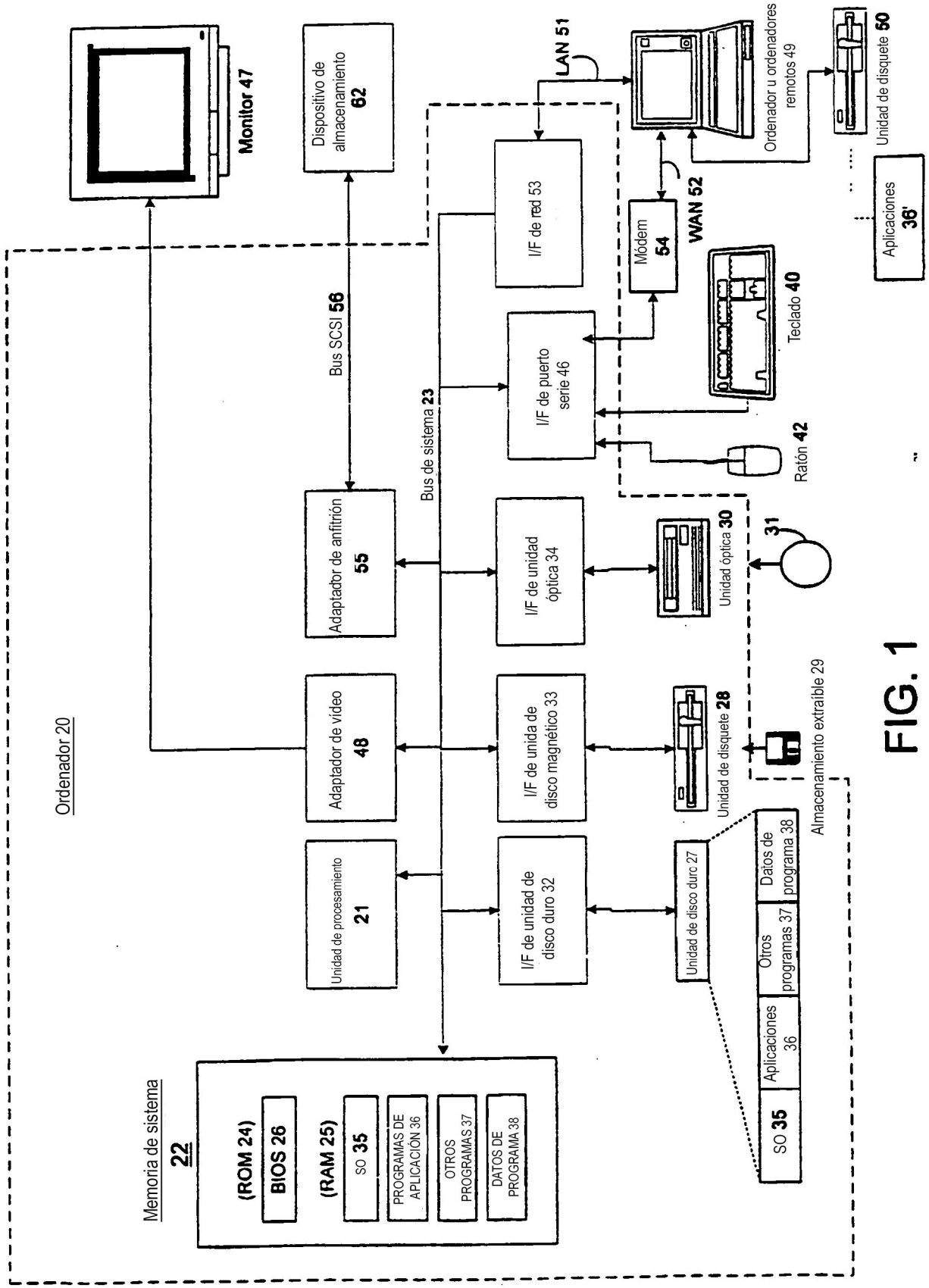

Ordenador 20
Monitor 47
Dispositivo de almacenamiento 62
LAN 51
Ordenador u ordenadores remotos 49
Unidad de disquete 60
Aplicaciones 36'
I/F de red 53
Módem 54
WAN 52
Bus SCSI 56
Bus de sistema 23
I/F de puerto serie 46
Teclado 40
Ratón 42
Adaptador de anfitrión 55
I/F de unidad óptica 34
Unidad óptica 30
31
Adaptador de vídeo 48
I/F de unida de disco magnético 33
Unidad de disquete 28
Almacenamiento extraíble 29
Unidad de procesamiento 21
I/F de unidad de disco duro 32
Unidad de disco duro 27
Datos de programa 38
Otros programas 37
Aplicaciones 36
SO 35
Memoria de sistema 22
(ROM 24)
BIOS 26
(RAM 25)
SO 35
PROGRAMAS DE APLICACIÓN 36
OTROS PROGRAMAS 37
DATOS DE PROGRAMA 38

FIG. 1

FIG. 2

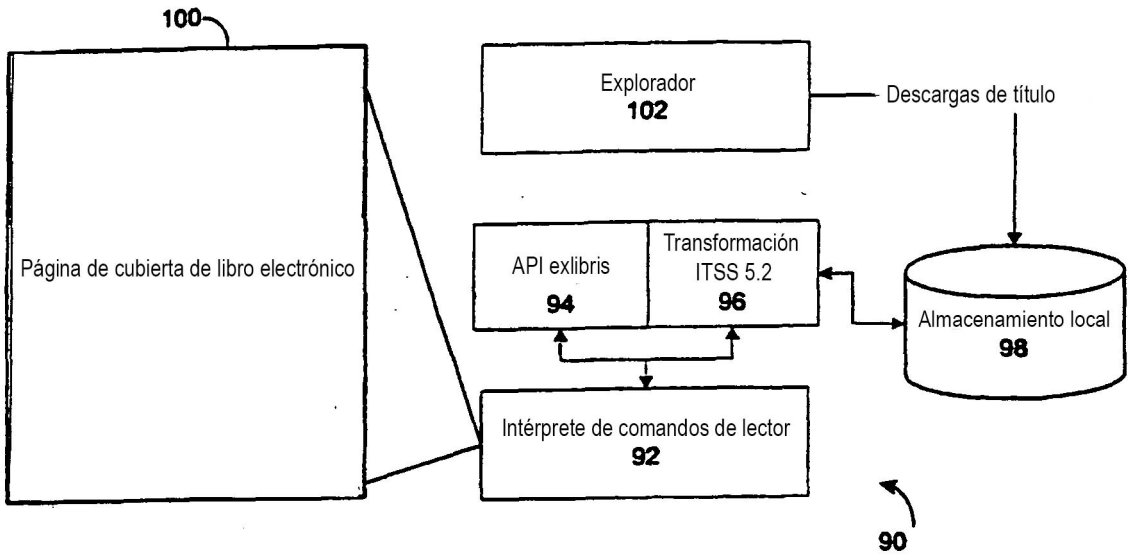

100
Página de cubierta de libro electrónico
Explorador
102
Descargas de título
API exlibris
94
Transformación
ITSS 5.2
96
Almacenamiento local
98
Intérprete de comandos de lector
92
90

FIG. 3

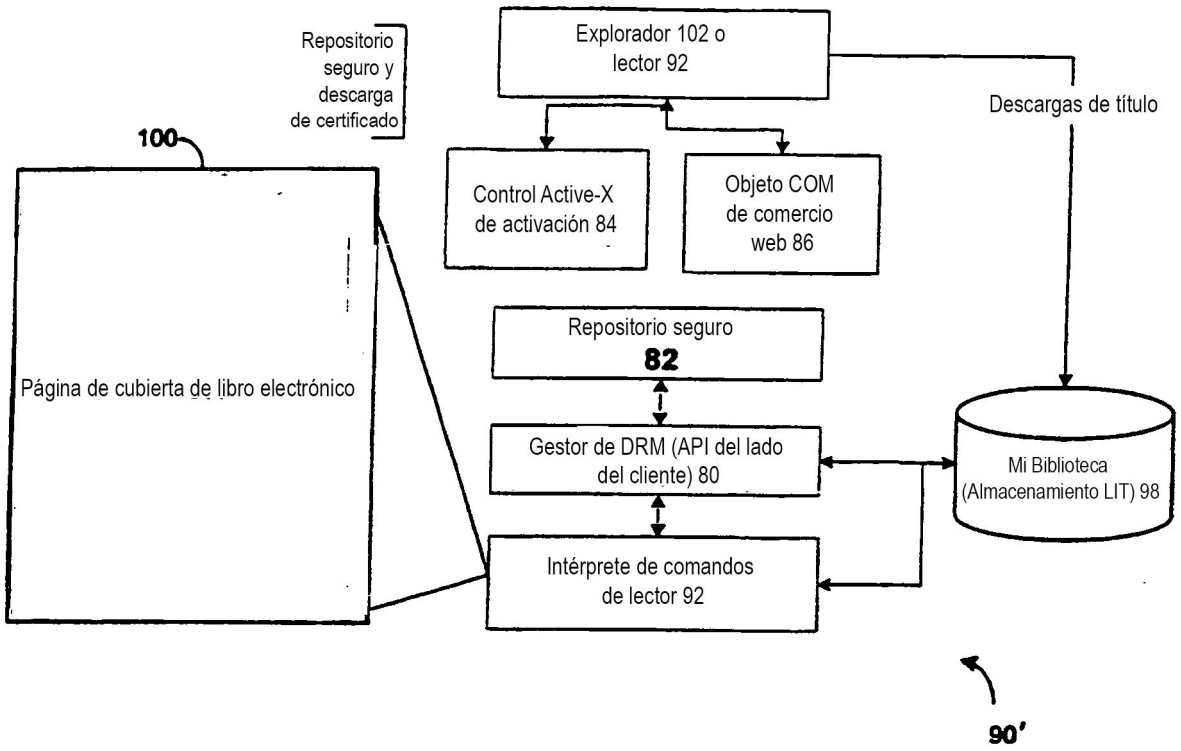

Repositorio seguro y descarga de certificado
Explorador 102 o lector 92
Descargas de título
100
Control Active-X de activación 84
Objeto COM de comercio web 86
Repositorio seguro 82
Página de cubierta de libro electrónico
Gestor de DRM (API del lado del cliente) 80
Mi Biblioteca (Almacenamiento LIT) 98
Intérprete de comandos de lector 92
90'

FIG. 4

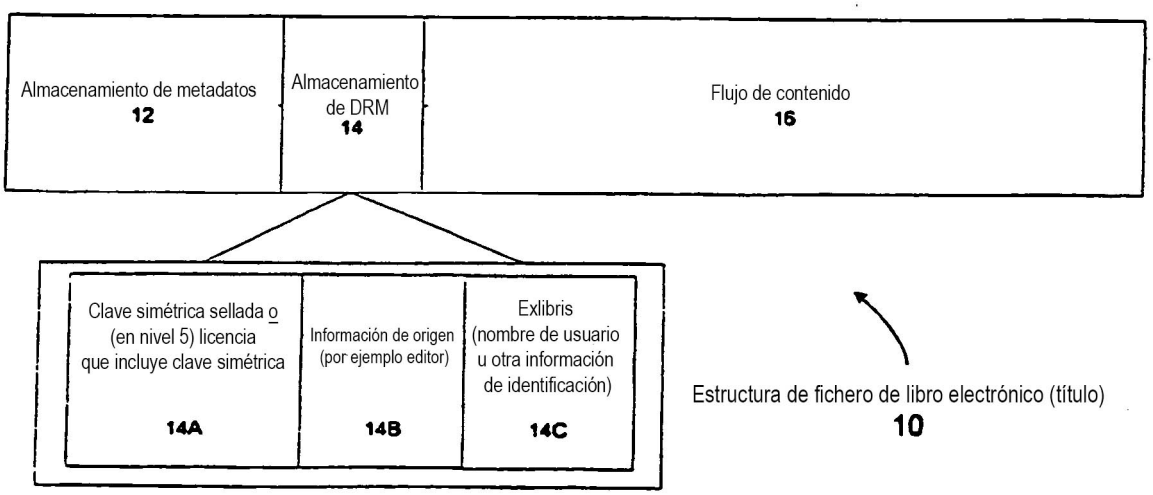

Almacenamiento de metadatos 12
Almacenamiento de DRM 14
Flujo de contenido 16
Clave simétrica sellada o (en nivel 5) licencia que incluye clave simétrica 14A
Información de origen (por ejemplo editor) 14B
Exlibris (nombre de usuario u otra información de identificación) 14C
Estructura de fichero de libro electrónico (título) 10

FIG. 5

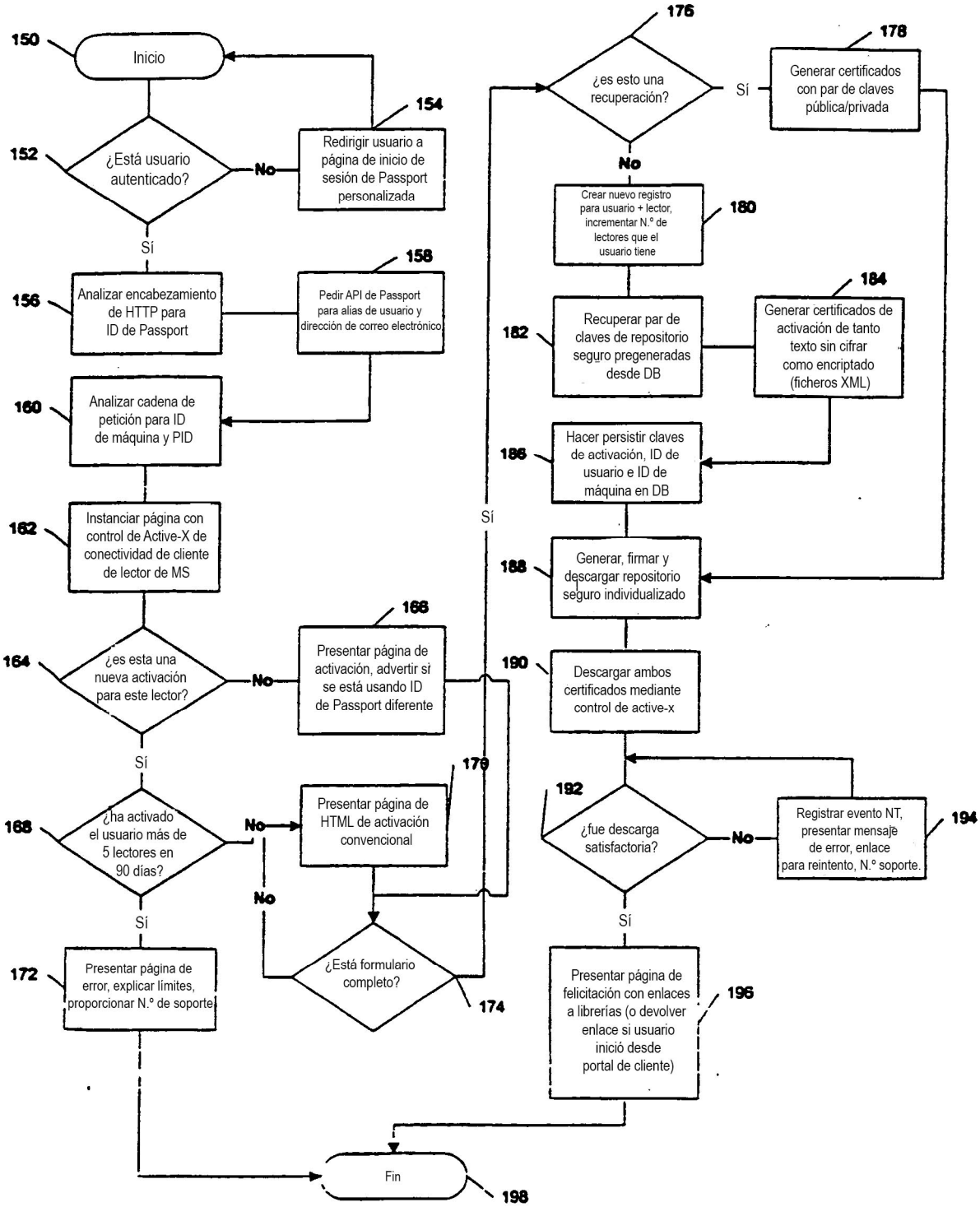
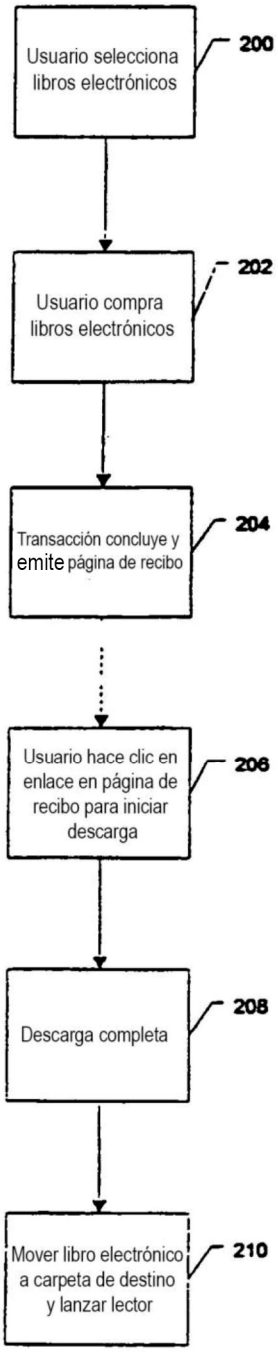

150
Inicio
152
¿Está usuario autenticado?
No
154
Redirigir usuario a página de inicio de sesión de Passport personalizada
Sí
156
Analizar encabezamiento de HTTP para ID de Passport
158
Pedir API de Passport para alias de usuario y dirección de correo electrónico
160
Analizar cadena de petición para ID de máquina y PID
162
Instanciar página con control de Active-X de conectividad de cliente de lector de MS
164
¿es esta una nueva activación para este lector?
No
166
Presentar página de activación, advertir si se está usando ID de Passport diferente
Sí
168
¿ha activado el usuario más de 5 lectores en 90 días?
No
170
Presentar página de HTML de activación convencional
Sí
172
Presentar página de error, explicar límites, proporcionar N.º de soporte
No
¿Está formulario completo?
174
Sí
175
¿es esto una recuperación?
Sí
178
Generar certificados con par de claves pública/privada
No
180
Crear nuevo registro para usuario + lector, incrementar N.º de lectores que el usuario tiene
182
Recuperar par de claves de repositorio seguro pregeneradas desde DB
184
Generar certificados de activación de tanto texto sin cifrar como encriptado (ficheros XML)
186
Hacer persistir claves de activación, ID de usuario e ID de máquina en DB
188
Generar, firmar y descargar repositorio seguro individualizado
190
Descargar ambos certificados mediante control de active-x
192
¿fue descarga satisfactoria?
No
194
Registrar evento NT, presentar mensaje de error, enlace para reintento, N.º soporte.
Sí
196
Presentar página de felicitación con enlaces a librerías (o devolver enlace si usuario inició desde portal de cliente)
Fin
198

FIG. 6


Usuario selecciona libros electrónicos
200
Usuario compra libros electrónicos
202
Transacción concluye y emite página de recibo
204
Usuario hace clic en enlace en página de recibo para iniciar descarga
206
Descarga completa
208
Mover libro electrónico a carpeta de destino y lanzar lector
210