(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 564 777**

(51) Int. CI.:

G06F 21/10 (2013.01)
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 00986344 (0)**

(97) Fecha y número de publicación de la concesión europea: **17.02.2016 EP 1242854**

(54) Título: **Comunicación entre servidores usando solicitud con parámetro cifrado**

(30) Prioridad:

17.12.1999 US 172318 P
17.12.1999 US 172319 P
27.06.2000 US 604944

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
29.03.2016

(73) Titular/es:

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

(72) Inventor/es:

DEMELLO, MARKO A.;
ZEMAN, PAVEL;
KRISHNASWAMY, VINAY y
BYRUM, FRANK D.

(74) Agente/Representante:

CARPINTERO LÓPEZ, Mario

DESCRIPCIÓN

Comunicación entre servidores usando solicitud con parámetro cifrado

Referencia cruzada a casos relacionados

La presente solicitud reivindica el beneficio de la solicitud provisional de EE. UU. con n.º 60/172.318 con título "*System for Distributing Content Having Multilevel Security Protection*", y la solicitud provisional de EE. UU. con n.º 60/172.319 con título "*System and Method for Digital Rights Management*", ambas presentadas el 17 de diciembre de 1999.

Campo de la invención

La presente invención se refiere, en general, al campo de la informática, y más en concreto a una técnica para comunicación entre servidores usando un tipo de solicitud que tiene un parámetro cifrado.

Antecedentes de la invención

Debido a que ha aumentado la disponibilidad y el uso de ordenadores y dispositivos electrónicos del tamaño de la palma, se ha vuelto común que los documentos se transmitan y se vean por medios electrónicos. Con la mejora de la comunicación a través de infraestructuras tales como Internet, existe un formidable impulso para proporcionar servicios y contenido potenciados a los dispositivos. Son ejemplos de servicios y contenido que se pueden proporcionar las obras de autor, tales como libros u otro material textual. La distribución electrónica de documentos de texto es tanto más rápida como más económica que la distribución convencional de copias en papel. El mismo principio es de aplicación a un contenido no textual, tal como audio y vídeo: la distribución electrónica de tal contenido es en general más rápida y más económica que la entrega de tal contenido en medios convencionales (por ejemplo, cinta magnética o disco óptico). No obstante, el bajo coste y la instantaneidad de la distribución electrónica, en combinación con la facilidad de copiar un contenido electrónico, están reñidos con el fin de una distribución controlada de una forma que proteja los derechos de los propietarios de las obras distribuidas.

Una vez que se ha transmitido un documento electrónico a una parte interesada, este se puede copiar y distribuir fácilmente a otros sin autorización por parte del propietario de los derechos en el documento electrónico o, con frecuencia, sin ni si siquiera el conocimiento del propietario. Este tipo de distribución ilícita de documentos puede privar de regalías y / o ingresos al autor o al proveedor de contenido. Un problema con muchos esquemas de entrega presentes es que estos pueden no hacer provisión alguna para proteger derechos de propiedad. Otros sistemas intentan proteger los derechos de propiedad, pero no obstante, son incómodos e inflexibles y hacen la visualización / lectura de las obras de autor (o la presentación de otro modo de las obras de autor, en el caso de un contenido no de texto tal como música, vídeo, etc.) difícil para el comprador.

Por lo tanto, a la vista de lo anterior, existe una necesidad de un sistema de gestión de derechos digitales mejorado que permita la entrega de obras electrónicas a compradores de una forma que proteja derechos de propiedad, al tiempo que también sea flexible y sencillo de usar. También existe una necesidad del sistema que proporcione unos niveles flexibles de protección de seguridad y sea operable en varias plataformas de cliente de tal modo que un contenido electrónico pueda ser visto / mostrado por su comprador en cada plataforma. El sistema de gestión de derechos digitales de la presente invención proporciona, de forma ventajosa, soluciones a los problemas anteriores los cuales protegen los derechos de propiedad intelectual de los propietarios de contenidos y permiten que los autores u otros propietarios de contenidos sean compensados por sus esfuerzos creativos, al tiempo que se garantiza que el mecanismo de protección no suponga una carga excesiva para los compradores.

El documento WO 96/42041 A se refiere al procesamiento de solicitudes de servicio de un cliente a un servidor a través de una red. En el sistema descrito, un servidor de contenido inicia la rutina de autorización mediante la redirección de la solicitud de un cliente hacia un servidor de autenticación que se puede encontrar en un hospedador diferente. El servidor de autenticación devuelve una respuesta para preguntar al cliente y, entonces, reenvía una nueva solicitud que consiste en el URL original al que se anexa una identificación de sesión (SID, *session identification*) al cliente en una redirección.

El documento WO 98/58306 A divulga un procedimiento y sistema para incorporar de forma segura una información electrónica a una aplicación de compra en línea.

Sumario de la invención

El objeto de la invención es la provisión de un procedimiento y un medio legible por ordenador mejorados para facilitar la distribución de contenido electrónico.

El presente objeto se soluciona mediante la invención tal como se reivindica en las reivindicaciones independientes.

Se definen realizaciones preferidas mediante las reivindicaciones dependientes.

Se proporciona una arquitectura de servidor, la cual soporta la distribución de contenido protegido en un sistema de gestión de derechos digitales ("DRM", *digital rights management*). La arquitectura incluye una disposición de servidor de activación, y una disposición de servidor de distribución. La arquitectura incluye diversas características de seguridad que protegen frente a la distribución no autorizada o el uso de contenido protegido, así como componentes de soporte lógico que implementan las características de seguridad.

De acuerdo con la arquitectura provista, el contenido se puede proteger en una pluralidad de niveles, incluyendo: sin protección, sellado por la fuente, sellado de forma individual (o "inscrito"), firmado por la fuente y completamente individualizado (o "exclusivo del propietario"). El contenido "sin protección" se distribuye en un formato no cifrado. El contenido "sellado por la fuente" y "sellado de forma individual" se cifra y se empaqueta con una clave de cifrado que se sella criptográficamente con determinados datos de gestión de derechos que están asociados con el contenido, de tal modo que la clave no se puede recuperar si se han alterado los datos de gestión de derechos. La distinción entre el sellado "por la fuente" e "individual" es que el contenido "sellado de forma individual" incluye en la información de datos de gestión de derechos pertinente para el propietario legítimo (por ejemplo, el nombre del propietario, el número de tarjeta de crédito, el número de recibo o el ID de transacción para la transacción de compra, etc.), de tal modo que esta información no se puede eliminar de una copia que funcione del contenido, previendo de ese modo la detección de distribuidores no autorizados. El tipo particular de información incluida es determinado por el comerciante minorista de la copia. El contenido "firmado" se firma criptográficamente de una forma tal que la aplicación de presentación puede verificar su autenticidad, o la autenticidad de su canal de distribución. El contenido "completamente individualizado" es un contenido cifrado provisto con una clave de descifrado que no ha sido meramente sellada con la información de gestión de derechos, sino también cifrada de una forma tal que no se puede acceder a esta en ausencia de un "repositorio seguro" y un "certificado de activación", los cuales son enviados por la disposición de servidor de activación solo a un cliente o conjunto de clientes particular, limitando de ese modo el uso de tal contenido a un número finito de instalaciones.

La disposición de servidor de activación incluye uno o más dispositivos informáticos de servidor los cuales "activan" dispositivos informáticos de cliente mediante la provisión de código y datos a estos dispositivos, en donde el código y los datos son necesarios para acceder a un contenido "completamente individualizado" en un dispositivo de cliente dado. En un ejemplo, los "datos" incluyen un certificado de activación que tiene una clave pública y una clave privada cifrada, y el "código" es un programa (por ejemplo, un "repositorio seguro") que accede a la clave privada en el certificado de activación mediante la aplicación, de una forma segura, de la clave necesaria para descifrar la clave privada cifrada. Preferiblemente, el par de claves en el certificado de activación está asociado de forma persistente con un "rol" autenticable, de tal modo que un dispositivo se puede "activar" para leer un contenido que se ha individualizado para ese rol, pero no un contenido que ha sido "completamente individualizado" para otros roles. Tal como se usa en el presente documento, un "rol" es un identificador único que puede estar unido a un usuario y puede ser autenticado de forma segura por un procedimiento fuera de banda - por ejemplo, un formulario de nombre de usuario y de contraseña en un navegador web para su uso a través de una capa de sockets segura (SSL, *secure socket layer*) es una realización a modo de ejemplo de un procedimiento de este tipo. Además, la disposición de servidor de activación preferiblemente proporciona un certificado de activación dado (es decir, un certificado de activación que tiene un par de claves particular) solo después de unas credenciales de autenticación (por ejemplo, un nombre de usuario y una contraseña) que estén asociadas con un rol. De acuerdo con una característica de la invención, el número de dispositivos que un rol particular puede activar puede estar limitado por tasa y o por número (por ejemplo, cinco activaciones dentro de un primer periodo de 90 días, seguido por una activación adicional durante cada periodo de 90 días posterior, hasta un máximo de diez activaciones), evitando de ese modo la proliferación no controlada de dispositivos en los que se puede presentar un contenido individualizado. Como un uso a modo de ejemplo de esta técnica, el contenido protegido se puede distribuir como un archivo que incluye un contenido que está cifrado con una clave simétrica, en donde la propia clave simétrica se proporciona por medio de una construcción de licencia que está incrustada en el archivo en un formulario cifrado por la clave pública del certificado, haciendo necesario tener, de este modo, tanto el certificado de activación como el repositorio seguro adjunto antes de interactuar con el contenido con licencia.

La disposición de servidor de distribución incluye uno o más servidores de comercio al por menor y uno o más sitios de cumplimiento. Los servidores de comercio al por menor venden contenido protegido (o dar de alta de otro modo a usuarios para recibir contenido protegido). Los sitios de cumplimiento proporcionan el contenido real que ha sido vendido por los servidores de comercio al por menor. El operador de un servidor de comercio al por menor puede ser una entidad diferente del operador de un sitio de cumplimiento, haciendo posible de ese modo que un comerciante minorista venda contenido protegido simplemente al pasar a formar parte de un acuerdo mediante el cual un sitio de cumplimiento proporcionará contenido vendido por el comerciante minorista. Esto permite que el comerciante minorista venda contenido sin invertir en los medios para almacenar o distribuir el contenido. En un ejemplo, el comerciante minorista y el sitio de cumplimiento acuerdan un secreto (por ejemplo, una clave criptográfica), y el comerciante minorista equipa su servidor con un soporte lógico que usa el secreto para crear una instrucción cifrada para proporcionar el contenido al comprador. Entonces, el comerciante minorista puede permitir que el comprador "dé cumplimiento" a su compra mediante la provisión de una solicitud de HTTP al comprador (por ejemplo, una solicitud de POST que se presenta como un hipervínculo en una página web de "recibo" o de "confirmación"), en donde la solicitud de HTTP contiene la dirección del sitio de cumplimiento y la instrucción cifrada. En el caso de un contenido que requiere un cierto nivel de individualización, la instrucción cifrada puede incluir la

información de individualización (por ejemplo, el nombre del comprador, o, en el caso del contenido "completamente individualizado", el certificado de activación del comprador). El sitio de cumplimiento recibe la instrucción cifrada cuando el comprador pulsa sobre el vínculo, y el sitio de cumplimiento usa el secreto compartido para descifrar la instrucción y proporcionar el contenido de acuerdo con la misma. Un objeto de modelo de objetos componentes (COM, *component object model*) se puede proporcionar al comerciante minorista el cual crea la instrucción cifrada.

El sitio de cumplimiento se puede organizar como un servidor de cumplimiento más uno o más servidores de "descarga" y un almacén de contenido. El almacén de contenido almacena un contenido que se va a distribuir a los consumidores. El servidor de cumplimiento mantiene unas bases de datos de información en relación con el cumplimiento de pedidos de contenido, tal como la ubicación física de artículos de contenido y el secreto (por ejemplo, la clave criptográfica) necesario para descifrar instrucciones que se reciben del comerciante minorista. Los servidores de descarga realizan la descarga real de contenido a consumidores / compradores del contenido, así como cualquier preparación del contenido que sea necesaria para dar cumplimiento a los requisitos de protección que están asociados con el contenido (por ejemplo, el servidor de descarga puede realizar una individualización del contenido). Cada servidor de descarga puede tener una memoria caché, en donde el servidor de descarga obtiene una copia de un artículo de contenido a partir del almacén de contenido (de acuerdo con la ubicación que se especifica en la base de datos de servidores de cumplimiento) la primera vez que se llama a ese servidor de descarga para procesar una descarga de ese artículo, en donde el servidor de descarga almacena el artículo en la memoria caché para futuras descargas. La memoria caché puede tener unos límites que están asociados con la misma, y esta puede expulsar los artículos fuera de la memoria caché en base a un algoritmo tal como un algoritmo de "uso menos reciente". El servidor de descarga también puede proporcionar una información que concierne a las descargas que este procesa al servidor de cumplimiento para la entrada en un registro. El servidor de descarga puede proporcionar esta información en forma de mensajes a través de una mensajería asíncrona, tal como la Cola de Mensajes de MICROSOFT (MSMQ, *MICROSOFT MESSAGE QUEUE*). El servidor de cumplimiento puede almacenar la información en una "base de datos de registro". Adicionalmente, cuando se realizan actualizaciones para la información almacenada en el servidor de cumplimiento que afecten al artículo de contenido que está almacenado en la memoria caché, el servidor de cumplimiento puede usar el servicio de mensajería para enviar mensajes a los diversos servidores de descarga indicando que el artículo se debería invalidar en las memorias caché de servidor de descarga.

Otras características de la invención se describen en lo sucesivo.

Breve descripción de los dibujos

El sumario anterior, así como la siguiente descripción detallada, se entiende mejor cuando se lee junto con los dibujos adjuntos. Para el fin de ilustrar la invención, números de referencia semejantes representan partes similares por la totalidad de las varias vistas de los dibujos, entendiéndose, no obstante, que la invención no se limita a las instrumentalidades y procedimientos específicos que se divulgan. En los dibujos:

la figura 1 es un formato de archivo de título de libro electrónico (*eBook*) a modo de ejemplo;
la figura 2 es un diagrama de bloques que muestra un entorno informático a modo de ejemplo en el que se pueden implementar unos aspectos de la presente invención;
la figura 3 es un diagrama de bloques de una realización de una primera arquitectura de servidor que implementa unos aspectos de un sistema de gestión de derechos digitales de acuerdo con la invención;
la figura 4 es un diagrama de bloques de una realización de una segunda arquitectura de servidor que implementa unos aspectos de un sistema de gestión de derechos digitales de acuerdo con la invención;
la figura 5 es un diagrama de bloques que ilustra determinadas interacciones dentro de un servidor de proveedor de contenido de acuerdo con unos aspectos de la invención;
la figura 6 es un diagrama de bloques que muestra componentes de una canalización de cumplimiento asíncrona de acuerdo con unos aspectos de la invención;
la figura 7 es un diagrama de flujo que ilustra el procedimiento de generar una licencia de acuerdo con unos aspectos de la invención;
la figura 8 es un diagrama de flujo que ilustra un procedimiento de activación de lector de cliente de acuerdo con unos aspectos de la invención; y
las figuras 9 y 10 son unos diagramas de flujo y de bloques que ilustran un flujo de comercio electrónico de acuerdo con unos aspectos de la invención.

Descripción detallada de la invención

La presente invención se dirige a un sistema para el procesamiento y la entrega de contenido electrónico en el que el contenido se puede proteger en múltiples niveles. Se describe una realización preferida de la invención, la cual se dirige al procesamiento y la entrega de libros electrónicos, no obstante, la invención no se limita a los libros electrónicos y puede incluir todo el contenido digital tal como vídeo, audio, ejecutables de soporte lógico, datos, etc.

Visión de conjunto

El éxito de la industria del libro electrónico requerirá, sin duda alguna, proporcionar al público comprador de libros existente una experiencia atractiva, segura y familiar para adquirir todo tipo de material textual. Este material puede incluir un material "gratuito" o de bajo coste que requiere poca protección frente a copia, a títulos de libros electrónicos de "calidad suprema" (en el presente documento "libros electrónicos") que requieren una protección de derechos exhaustiva. Con el fin de posibilitar una transición fluida desde el modelo actual de distribución y de comercio al por menor para libros impresos a un sistema de distribución electrónica, ha de existir una infraestructura para asegurar un alto nivel de protección frente a copia para aquellas publicaciones que lo demanden, al tiempo que se soporta la distribución de títulos que requieren unos niveles de protección inferiores.

Los sistemas de gestión de derechos digitales (DRM, *Digital Rights Management*) y de servidor de activos digitales (DAS, *Digital Asset Server*) de la presente invención proporcionan de forma ventajosa una infraestructura de este tipo. La presente invención hace la compra de un libro electrónico más deseable que la "sustracción" (por ejemplo, hacer una copia no autorizada) de un libro electrónico. El sistema de DRM no intrusivo reduce al mínimo el riesgo de piratería, al tiempo que se aumenta la probabilidad de que cualquier piratería sea compensada por un aumento en las ventas / la distribución de libros en forma de libros electrónicos. Además, la presente invención provee a los comerciantes minoristas con un sistema que se puede implementar rápidamente con un coste bajo.

Los usuarios primarios del sistema de DRM son editores y comerciantes minoristas, los cuales usan y / o implementan el sistema de DRM para asegurar la legitimidad del contenido vendido así como protección frente a copia. Usuarios a modo de ejemplo del sistema de DRM pueden ser el editor tradicional, el editor "de vanguardia", y el "autor hambriento". Es probable que el editor tradicional esté preocupado por la pérdida de ingresos procedentes de su operación de publicación de libros impresos ante la piratería de libros electrónicos. El editor de vanguardia no está necesariamente preocupado con los incidentes aislados de piratería y puede apreciar que el comercio de libros electrónicos tendrá mucho éxito en un sistema en el que los consumidores desarrollen hábitos de compra. Al mismo tiempo, el autor hambriento, al cual podría gustarle recoger fondos para la venta de sus obras, está más interesado en la atribución (por ejemplo, que el nombre del autor esté enlazado de forma permanente a la obra).

Tal como se describirá con mayor detalle en lo sucesivo, el sistema de DRM de la presente invención logra sus fines mediante la protección de obras, al tiempo que se posibilita su uso legítimo por los consumidores, al soportar diversos "niveles" de protección. En el nivel más bajo ("el nivel 1"), el proveedor y / o la fuente de contenido puede elegir sin protección por medio de libros electrónicos no firmados y no sellados (de texto no cifrado) que no incluyen una licencia. Un nivel siguiente de protección ("el nivel 2") es "sellado por la fuente", lo que quiere decir que el contenido se ha cifrado y sellado con una clave, en donde el sello se realiza usando una función criptográfica de troceo de los metadatos del título del libro electrónico (véase más adelante) y la clave es necesaria para descifrar el contenido. El sellado en fuente protege frente a la manipulación indebida del contenido o sus metadatos adjuntos después de que se haya sellado el título, debido a que cualquier cambio en los metadatos hará que el título se vuelva inutilizable; no obstante, el sellado en fuente no garantiza la autenticidad de una copia del título (es decir, el sellado en fuente no proporciona un mecanismo para distinguir copias legítimas de copias no autorizadas). En el caso del "autor hambriento", el nombre del autor se puede incluir en los metadatos para un enlace permanente al contenido, satisfaciendo de ese modo el fin de atribución del "autor hambriento". Un nivel siguiente de protección ("el nivel 3") es "sellado de forma individual" (o "inscrito"). Un título "sellado de forma individual" es un libro electrónico cuyos metadatos incluyen una información en relación con el comprador legítimo (por ejemplo, el nombre o el número de tarjeta de crédito del usuario, el ID de transacción o el número de recibo procedente de la transacción de compra, etc.), de tal modo que esta información está enlazada criptográficamente al contenido cuando se sella el título. Este nivel de protección desalienta la distribución de copias del título por parte de personas, debido a que sería fácil detectar el origen de una copia no autorizada (y cualquier cambio en los metadatos, incluyendo la información en relación con el comprador, haría imposible, o al menos improbable, que se pudiera eliminar el sello de la clave de descifrado necesaria).

El nivel siguiente de protección ("el nivel 4") es "firmado por la fuente". Los libros electrónicos firmados por la fuente son títulos que pueden ser autenticados por un "lector" (el cual, tal como se analiza más en concreto en lo sucesivo, es una aplicación de usuario que posibilita la lectura de libros electrónicos en un dispositivo informático, tal como un PC, un ordenador portátil, un Asistente Digital Personal (PDA, *Personal Digital Assistant*), PocketPC, o un dispositivo de lectura construido especialmente). La autenticidad se puede definir preferiblemente en tres variedades: "firmado por herramienta", la cual garantiza que el título de libro electrónico fue generado por una herramienta de conversión y de cifrado de confianza; "firmado por el propietario", la cual es un libro electrónico firmado por herramienta que también garantiza la autenticidad del contenido en la copia (por ejemplo, el propietario puede ser el autor u otro titular de derechos de autor); y "firmado por el proveedor", la cual es un libro electrónico firmado por herramienta que avala la autenticidad de su proveedor (por ejemplo, el editor o comerciante minorista del contenido). La "herramienta", el propietario y el proveedor pueden tener, cada uno, su propio par de claves asimétricas para facilitar la creación y la validación de firmas digitales de la información. Un título puede ser tanto firmado por el proveedor como firmado por la fuente, lo cual 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 del propietario" ("el nivel 5"). Los títulos "completamente individualizados" solo pueden ser abiertos por aplicaciones de lector autenticado que se "activan" para un usuario particular, protegiendo de ese modo frente a la

migración de un título del lector (o lectores) de una persona a un lector que no está registrado con esa persona. Con el fin de que el lector de la presente invención abra un título que está protegido en el nivel 5, el Lector se ha de "activar" (es decir, el dispositivo en el que reside el lector ha de tener un certificado de activación para un rol particular, y un repositorio seguro). El procedimiento de activación se describe con mayor detalle en lo sucesivo con referencia a la figura 8.

Los sistemas de la presente invención también definen una arquitectura para compartir una información entre un lector, un proveedor de contenido y una fuente de contenido, cómo se usa esa información para "sellar" títulos en los diversos niveles, y cómo ha de estar estructurada esa información. La disponibilidad de estas elecciones posibilitará que las fuentes de contenido escojan y elijan qué contenido será vendido a qué usuarios y usando qué protección (de haber alguna). La información particular se puede usar para firmar y / o sellar títulos para su uso por un lector, y un lector compatible (el cual, en el caso del nivel 5, puede ser un lector que está activado para un rol particular) puede eliminar el sello del título y habilitar la lectura del libro electrónico.

Estructura de archivos de libro electrónico

El sistema de DRM de la presente invención protege contenido mediante la incorporación del mismo en una estructura de archivo, tal como la estructura a modo de ejemplo que se muestra en la figura 1. Haciendo referencia a la figura 1, el libro electrónico 10 contiene un contenido 16, el cual es un texto tal como un libro (o cualquier contenido electrónico) que ha sido cifrado por una clave (la "clave de contenido"), la cual se ha, en sí misma, cifrado y / o sellado. En una realización preferida, la clave es una clave simétrica 14A que se sella con una función criptográfica de troceo de unos metadatos 12 o, en el caso de los títulos de nivel 5, con la clave pública del certificado de activación del usuario. Esta clave se almacena o bien como una secuencia separada en una sección de subalmacenamiento del archivo de libro electrónico (el Almacenamiento de DRM 14 en el diagrama) o bien, en el caso de los títulos de nivel 5, en la licencia. (En el caso de los títulos de nivel 5, en lugar de almacenar la clave de contenido como una secuencia separada, la secuencia 14A contiene una licencia, la cual es una construcción que define los derechos que puede ejercer el usuario tras la compra del título. En los títulos que tienen una licencia, la clave de contenido está contenida dentro de la licencia.). También están incluidos en el almacenamiento de DRM 14 la secuencia de fuente 14B, la cual puede incluir el nombre del editor (o otra fuente de contenido), así como el tren de exlibris 14C, el cual, para los títulos sellados de forma individual (el nivel 3 y / o el nivel 5), incluye el nombre del consumidor tal como es provisto por el comerciante minorista (el cual, por ejemplo, se puede obtener como parte de la transacción comercial de compra de un libro electrónico 10, tal como a partir de la información de tarjeta de crédito del consumidor). El procedimiento de calcular la función criptográfica de troceo que cifra y / o sella la clave simétrica 14C (o el procedimiento de usar tal función criptográfica de troceo para sellar la clave) es preferiblemente un "secreto" que solo es conocido por unas herramientas de preparación de contenidos de confianza y aplicaciones de presentación de confianza. El uso de una función de troceo de esta forma puede complicar / desalentar la manipulación indebida de los metadatos 12 que están contenidos en el libro electrónico 10. Se hace notar que se puede usar cualquier procedimiento para "sellar" un libro electrónico, siempre que tal procedimiento proporcione una cierta medida de resistencia a manipulación indebida al libro electrónico 10.

De acuerdo con la presente invención, los metadatos 12 pueden incluir una etiqueta de derechos de autor, la cual describe los derechos que con concedidos al usuario o comprador por la fuente de contenido (por ejemplo, el editor). Siempre que se encuentre presente tal etiqueta, el cliente (por ejemplo, el dispositivo 90 o 92 que se muestra en la figura 4) puede presentar visualmente a un usuario el texto que está incluido en la etiqueta. Se apreciará que el acto de recordar a los usuarios las leyes de propiedad intelectual que sean de aplicación a sus libros electrónicos puede servir para desalentar que los usuarios típicos intenten copiar libros electrónicos.

Arquitectura del sistema de DRM

Tal como se muestra en la figura 2, un sistema a modo de ejemplo para implementar la invención incluye un dispositivo informático de propósito general en la forma de un ordenador personal o servidor de red 20 convencional o similares, incluyendo una unidad de procesamiento 21, una memoria de sistema 22, y un bus de sistema 23 que acopla diversos componentes de sistema incluyendo la memoria de sistema 22 con la unidad de procesamiento 21. El bus de sistema 23 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 que usa cualquiera de una variedad de arquitecturas de bus. La memoria de sistema incluye una memoria de solo lectura (ROM, *read-only memory*) 24 y una memoria de acceso aleatorio (RAM, *random access memory*) 25. Un sistema básico de entrada / salida 26 (BIOS, *basic input / output system*), que contiene las rutinas básicas que ayudan a transferir información entre elementos dentro del ordenador personal 20, tal como durante el arranque, está almacenado en la ROM 24. El ordenador personal o servidor de red 20 puede incluir adicionalmente una unidad de disco duro 27 para leer de y escribir en un disco duro, que no se muestra, una unidad de disco magnético 28 para leer de o escribir en un disco magnético extraíble 29, y una unidad de disco óptico 30 para leer de o escribir en un disco óptico extraíble 31 tal como un CD-ROM u otros medios ópticos. La unidad de disco duro 27, la unidad de disco magnético 28 y la unidad de disco óptico 30 están conectadas con el bus de sistema 23 mediante una interfaz de unidad de disco duro 32, una interfaz de unidad de disco magnético 33, y una interfaz de unidad óptica 34, de forma respectiva. Las unidades y sus medios legibles por ordenador asociados proporcionan un almacenamiento no volátil de instrucciones legibles por ordenador, estructuras de datos, módulos de programa y otros datos para el ordenador personal o servidor de red 20. A pesar de que el

entorno a modo de ejemplo que se describe en el presente documento emplea un disco duro, un disco magnético extraíble 29 y un disco óptico extraíble 31, debería ser apreciado por los expertos en la materia que otros tipos de medios legibles por ordenador los cuales pueden almacenar unos datos a los que puede acceder un ordenador, tales como casetes magnéticos, tarjetas de memoria flash, discos de vídeo digital, cartuchos de Bernoulli, memorias de acceso aleatorio (RAM), memorias de solo lectura (ROM) y similares también se pueden usar en el entorno operativo a modo de ejemplo.

Un número de módulos de programa se pueden almacenar en el disco duro, el disco magnético 29, el disco óptico 31, la ROM 24 o la RAM 25, incluyendo un sistema operativo 35 (por ejemplo, Windows® 2000, Windows NT®, o Windows 95 / 98), uno o más programas de aplicación 36, otros módulos de programa 37 y datos de programa 38. Un usuario puede introducir comandos e información en el ordenador personal 20 a través de dispositivos de entrada tales como un teclado 40 y un dispositivo señalador 42. Otros dispositivos de entrada (que no se muestran) pueden incluir un micrófono, una palanca para juegos, un controlador para juegos, un disco de satélite, scanner o similares. Con frecuencia, estos y otros dispositivos de entrada están conectados con la unidad de procesamiento 21 a través de una interfaz de puerto serie 46 que está acoplada con el bus de sistema 23, pero se pueden conectar mediante otras interfaces, tal como un puerto paralelo, un puerto de juegos, un bus serie universal (USB, *universal serial bus*), o un puerto serie de alta velocidad 1394. Un monitor 47 u otro tipo de dispositivo de presentación visual también está conectado con el bus de sistema 23 por medio de una interfaz, tal como un adaptador de vídeo 48. Además del monitor 47, los ordenadores personales por lo general incluyen otros dispositivos de salida periféricos (que no se muestran), tales como altavoces e impresoras.

El ordenador personal o servidor de red 20 puede operar en un entorno de red usando unas conexiones lógicas con uno o más ordenadores remotos, tal como un ordenador remoto 49. El ordenador remoto 49 puede ser otro ordenador personal, otro servidor de red, un encaminador, un PC de red, un dispositivo del mismo nivel u otro nodo de red común, y por lo general incluye muchos o la totalidad de los elementos que se han descrito en lo que antecede en relación con el ordenador personal 20, a pesar de que solo un dispositivo de almacenamiento en memoria 50 se ha ilustrado en la figura 2. Las conexiones lógicas que se muestran en la figura 2 incluyen una red de área local (LAN, *local area network*) 51 y una red de área extensa (WAN, *wide area network*) 52. Tales entornos de red son comunes en oficinas, redes informáticas a nivel de empresa, Intranets e Internet.

Cuando se usa en un entorno de red de LAN, el ordenador personal o servidor de red 20 está conectado con la red local 51 a través de un adaptador o interfaz de red 53. Cuando se usa en un entorno de red de WAN, el ordenador personal o servidor de red 20 por lo general incluye un módem 54 u otros medios para establecer comunicaciones a través de la red de área extensa 52, tal como Internet. El módem 54, el cual puede ser interno o externo, está conectado con el bus de sistema 23 por medio de la interfaz de puerto serie 46. En un entorno de red, los módulos de programa que se muestran en relación con el ordenador personal o servidor de red 20, o porciones de los mismos, se pueden almacenar en el dispositivo de almacenamiento en memoria remoto 50. Se apreciará que las conexiones de red que se muestran son a modo de ejemplo y se pueden usar otros medios de establecimiento de un vínculo de comunicaciones entre los ordenadores.

Arquitectura de servidor

Haciendo referencia a continuación a la figura 3, en ella se ilustra una primera arquitectura de servidor 70 a modo de ejemplo que implementa el sistema de DRM de la presente invención. La arquitectura de servidor 70 se implementa y se despliega en, por ejemplo, un sitio de comercio al por menor / distribución. En una realización de la invención, todos los componentes de arquitectura de servidor 70 están asociados con una única parte interesada (por ejemplo, una gran librería de libros electrónicos) que tanto comercia al por menor con los libros electrónicos 10 como realiza la descarga real de los libros electrónicos 10 en los dispositivos de lectura de los clientes. En otra realización de la invención, los servidores de librería 72 y el objeto de COM de cifrado de URL 74 están asociados con una parte interesada (por ejemplo, un comerciante minorista de los libros electrónicos 10 que no realiza descargas), y los otros componentes de arquitectura de servidor 70 están asociados con una segunda parte interesada (por ejemplo, una "casa de cumplimiento"), la cual realiza descargas de los libros electrónicos 10 que vende / con los que comercia al por menor la primera parte interesada.

Las funciones que son provistas por la arquitectura de servidor 70 incluyen: cifrado de libros electrónicos de origen, conversión al formato de lector objetivo, generación de la construcción de licencia que define los derechos que se conceden al usuario (en los títulos de nivel 5), sellado del contenido antes de la descarga de acuerdo con unos requisitos (por ejemplo, un nivel de protección) que son expuestos por el proveedor de publicaciones, y descarga de títulos de libros electrónicos. Esta arquitectura de servidor también incluye unas características que prevén una configuración flexible que posibilita que los usuarios de esta tecnología (proveedores de contenido, comerciantes minoristas) adapten la escala de su sistema de acuerdo con sus necesidades. Estas características incluyen: resolución dinámica (a través de una consulta de base de datos) de ID de archivo en ubicaciones físicas de archivo, el almacenamiento en memoria cache de las descargas más populares para una eficiencia más elevada y un mejor rendimiento (en donde la memoria caché puede expulsar los artículos en base a, por ejemplo, una función de uso menos reciente), y el registro asíncrono de cada archivo descargado (también en una base de datos) para fines de auditoría / notificación y / o facturación posteriores. Otras funciones pueden ser realizadas por la arquitectura de servidor 70 de acuerdo con la presente invención.

Los servidores de librería 72 son, preferiblemente, servidores de tipo servidor de Información de Internet de MICROSOFT® (IIS, *Internet Information Server*) implementados en un servidor de red, tal como el ordenador 20 que se ilustra en la figura 2. Los servidores de librería 72 se pueden comunicar con los usuarios por medio de un soporte lógico de navegación web (por ejemplo, mediante la provisión de páginas web para su visualización con un navegador INTERNET EXPLORER de MICROSOFT o un navegador NETSCAPE NAVIGATOR). A través de esta comunicación, los servidores de librería 72 pueden permitir que los usuarios compren títulos de libros electrónicos, establezcan su relación de pertenencia con el comerciante minorista, paguen por sus transacciones y accedan a unas páginas de prueba de compra (recibos de lado de servidor). El objeto de cifrado de URL 74 puede residir en los servidores de librería 72. El objeto de cifrado de URL 74 cifra un conjunto de parámetros en relación con un libro electrónico 10 que se ha comprado en el servidor de librería 72. El objeto de cifrado de URL 74 puede cifrar estos parámetros usando un secreto (por ejemplo, una clave criptográfica simétrica) compartido entre el servidor de librería 72 y el servidor de contenido web 76. Por ejemplo, los parámetros pueden incluir una identificación del libro electrónico comprado, una información acerca de la compra tal como el nombre o el número de tarjeta de crédito del comprador o un ID de transacción (por ejemplo, en el caso de los títulos de nivel 3 o 5), y una marca de tiempo. Será apreciado por los expertos en la materia que los parámetros que se enumeran en lo que antecede son a modo de ejemplo, y se podrían usar diferentes parámetros sin apartarse del ámbito de la invención. Los parámetros cifrados se pueden incluir en una solicitud de HTTP que señala el servidor de contenido web 76, de tal modo que el servidor de contenido 76 puede dar cumplimiento a la compra realizada en el servidor de librería 72. Por ejemplo, después de que un libro electrónico 10 haya sido seleccionado por un comprador, el servidor de librería 72 podría subir al dispositivo informático del comprador una página web que contiene un vínculo que está asociado con una solicitud de POST, en donde la solicitud de POST señala un servidor de contenido tal como "www.content-provider.com", y el cuerpo del POST contiene los parámetros cifrados. En una realización alternativa de la invención, el vínculo que se proporciona en la página web se podría asociar con una solicitud de GET, tal como "*http://www.content-provider.com/isapi/_ds.dll?action=download&value=<parámetros_cifrados>*", a pesar de que la presente realización alternativa tiene la desventaja de que algunos navegadores imponen un límite sobre el tamaño aceptable de un URL (por ejemplo, 2 kilobytes), restringiendo de ese modo el tamaño de los parámetros cifrados. Cualquiera que sea el tipo de solicitud de HTTP que está asociada con el vínculo, entonces el usuario podría seguir el vínculo para iniciar la descarga. Debido a que los parámetros se han cifrado con un secreto compartido entre el servidor de librería 72 y el servidor de contenido 76, es posible que el servidor de contenido 76 verifique que los parámetros cifrados se originaron en un servidor de librería legítimo 72 (por ejemplo, uno para el cual el operador del servidor de contenido 76 ha acordado proporcionar servicios de descarga). Si se incluye una marca de tiempo, entonces el servidor de contenido 76 puede usar la marca de tiempo para asegurar que los parámetros cifrados se generaron recientemente, resistiendo de ese modo los "ataques de reproducción" (es decir, al "husmear" la solicitud de HTTP una persona que desea descargar libros electrónicos que no ha comprado de forma legítima). El objeto de cifrado de URL 74 se implementa preferiblemente como un objeto de COM de lado de servidor, y se instancia preferiblemente por medio de Páginas de Servidor Activo (ASP, *Active Server Pages*).

Los servidores de contenido 76 son preferiblemente unos servidores IIS que se implementan en un servidor de red (preferiblemente, diferente del servidor de librería 72). Al igual que con el servidor de librería 72, el servidor de contenido 76 se puede implementar en un ordenador tal como el ordenador 20 que se muestra en la figura 2. Se proporciona una extensión de ISAPI de servidor de descarga 78, la cual es una DLL de extensión de IIS que preferiblemente entrega las solicitudes entrantes a los servidores de contenido 76. La DLL de ISAPI 78 es responsable de la validación de las solicitudes de descarga, la recuperación del archivo de libro electrónico apropiado 10 del almacén de contenido 80 por medio del módulo de complemento de almacén de contenido 88, el sellado individual de las copias, la devolución de los títulos de libros electrónicos 10 a los usuarios finales y el registro de la transacción en la base de datos de cumplimiento 84 por medio de un módulo de mensajería asíncrona. El cliente independiente de Cola de Mensajes de MICROSOFT (MSMQ, *MICROSOFT Message Queue*) 86 es un módulo de mensajería asíncrona a modo de ejemplo que se puede usar en la arquitectura de servidor 70 (y la arquitectura de servidor 70' que se muestra en la figura 4 y que se analiza en lo sucesivo). A pesar de que el uso de la tecnología de MSMQ de Microsoft es preferible para una comunicación asíncrona de sus mensajes de servidor a servidor (el cliente de MSMQ 86), será apreciado por los expertos en la materia que se puede usar cualquier tecnología de mensajería de almacenamiento y reenvío. De acuerdo con un aspecto de la arquitectura de servidor 70 (y la arquitectura 70'), tal tecnología de mensajería flexible se puede usar para lograr altos grados de fiabilidad y escalabilidad, debido a que toda la mensajería de servidor a servidor que no requiere unas comunicaciones en tiempo real se lleva a cabo usando una canalización de comunicación asíncrona.

El almacén de contenido 80 es preferiblemente un sistema de gestión de bases de datos o sistema de archivos grande y unido a red (o una pluralidad de tales sistemas de archivos o sistemas de gestión de bases de datos). El almacén de contenido 80 sirve como un repositorio para títulos de LIT (los libros electrónicos 10) que son usados por la ISAPI de servidor de descarga 78 cuando se da cumplimiento a pedidos de los libros electrónicos 10. El almacén de contenido 80 preferiblemente expone una trayectoria de convención de nomenclatura universal (UNC, *Universal Naming Convention*) a la que puede acceder la ISAPI de servidor de descarga 78. Por razones de seguridad, es preferible que el almacén o almacenes de contenido 80 existan por detrás de un cortafuegos y que no estén expuestos directamente a Internet. La herramienta de gestión y de cifrado de contenidos 82 es un componente que realiza unas funciones tales como convertir contenido al formato de LIT (por ejemplo, el libro electrónico 10), cifrar y sellar cada título de libro electrónico en el almacén de contenido 80. La herramienta de gestión y de cifrado de

contenidos 82 también actualiza la base de datos de cumplimiento 84 con la ubicación física de cada archivo de LIT en el almacén de contenido 80, el cual se pone en correspondencia con su ID único en la base de datos de cumplimiento 84. La herramienta 82 acepta archivos de fuente de texto no cifrado (LIT, OEB, HTML, etc.) y genera archivos de LIT cifrados que son sellados por la fuente (por ejemplo, el nivel 2), para la posterior recuperación por la ISAPI de servidor de descarga 78.

Haciendo referencia a continuación a la figura 4, en ella se ilustra una segunda arquitectura de servidor 70' de acuerdo con la presente invención. La arquitectura de servidor 70' es un modelo distribuido, e incluye tres centros de datos: un sitio de comercio al por menor 71, un sitio de DRM y de cumplimiento 73, y un sitio de activación 75. Al igual que con la arquitectura de servidor 70, el comercio al por menor de contenido y el cumplimiento de pedidos de contenido pueden ser realizados por una única parte interesada, o una primera parte interesada puede comerciar al por menor con los libros electrónicos 10 al tiempo que una segunda parte interesada da cumplimiento a unos pedidos de los libros electrónicos 10 que fueron vendidos por la primera parte interesada. En este último escenario, el sitio de comercio al por menor 71 está asociado con la primera parte interesada, y el sitio de DRM y de cumplimiento 73 está asociado con la segunda parte interesada. Dentro de la arquitectura de la figura 4, es preferible que todas las aplicaciones basadas en servidor web estén agrupadas por detrás de una dirección de IP virtual, y que los servidores de contenido sean de doble alojamiento. También es preferible que los servidores de activación 94 se basen en el sistema de pertenencia de PASSPORT™ de MICROSOFT® para asociar unos certificados de activación con roles de usuario final, tal como se describirá en lo sucesivo (a pesar de que PASSPORT es meramente a modo de ejemplo de una autoridad de espacio de nombres que se puede usar para este fin).

Lo siguiente es una breve descripción de los componentes de la arquitectura de servidor 70'. Los servidores de librería 72 que están asociados con el sitio de comercio al por menor 71 son servidores de red que se implementan en un ordenador tal como el ordenador 20. Preferiblemente, los servidores de librería 72 ejecutan Servidores Avanzados de WINDOWS® 2000 que ejecutan IIS. Al igual que en la arquitectura 70, estos servidores alojan el sitio web comercial que permite que los usuarios realicen acciones tales como comprar títulos de libros electrónicos, establecer su relación de pertenencia con el comerciante minorista, pagar sus transacciones y / o acceder a las páginas de prueba de compra (recibos de lado de servidor). El objeto de cifrado de URL 74 se proporciona para la integración en el sitio de comerciante minorista 71. Al igual que en la arquitectura de servidor 70, el objeto de cifrado de URL 74 de la arquitectura de servidor 70' se puede implementar como un objeto de COM de lado de servidor instalado en los servidores de librería 72 e instanciado por medio de páginas ASP, y este puede cifrar unos parámetros en relación con la compra de un libro electrónico 10 de tal modo que el servidor de contenido 76 puede validar los parámetros cifrados, autenticar al comerciante minorista por medio de un secreto compartido (por ejemplo, una clave simétrica que se usa para cifrar los parámetros), evitar los ataques de reproducción, y determinar el contenido a descargar a los usuarios finales.

El servidor o servidores de contenido / servidor o servidores de descarga 76 son preferiblemente Servidores Avanzados de WINDOWS® 2000 que ejecutan IIS. Los servidores de contenido / servidores de descarga 76 alojan las partes esenciales de la aplicación de cumplimiento de DAS, incluyendo la extensión de ISAPI de servidor de descarga 78, el módulo de complemento de almacén de contenido 88, el módulo de servidor de licencia 77 y el cliente de canalización de cumplimiento 86.

Tal como se ha hecho notar en lo que antecede, la extensión de ISAPI de servidor de descarga 78 es preferiblemente una DLL de extensión de IIS que entrega las solicitudes entrantes a los servidores de contenido 76. Esta es responsable de la validación de cada solicitud de descarga, el sellado individual de las copias (cuando sea necesario), la solicitud de una licencia para copias completamente individualizadas (es decir, de nivel 5) de libros electrónicos, la devolución de los títulos de libros electrónicos a los usuarios finales y el registro de la transacción de descarga en una base de datos, tal como la base de datos de registro 91.

El módulo de complemento de almacén de contenido 88 es preferiblemente una DLL la cual es responsable de la determinación de la ubicación física en el almacén de contenido 88 de cada uno de los archivos de LIT (libros electrónicos) que se están descargando, en base a una combinación de parámetros (por ejemplo, parámetros de ID de libro y de tipo de ID de libro) que están incluidos en la solicitud de descarga (es decir, los parámetros cifrados unidos al URL). El módulo de complemento 88 también recupera, de la base de datos de cumplimiento 89, una información de configuración (por ejemplo, el certificado de clave pública y la clave privada del emisor de licencia, una lista de comerciantes minoristas soportados y sus claves simétricas, etc.) que se requiere para arrancar la DLL de extensión de ISAPI de servidor de descarga 78.

El módulo de servidor de licencia 77 es un subcomponente de la DLL de extensión de ISAPI de servidor de descarga 78. Este es responsable de la generación y el sellado de licencias para los archivos de LIT con protección de nivel 5. Tal como se describe más plenamente en lo sucesivo, una licencia es una construcción que define los derechos que los derechos que puede ejercer el usuario tras la compra de un título de libro electrónico. El módulo de servidor de licencia 77 también valida el certificado de activación del usuario al cual se está descargando el libro electrónico y firma cada licencia con la clave privada del proveedor de centro de cumplimiento, lo cual permitirá más adelante que el lector 90 o 92 autentique el canal de distribución cuando se acceda al archivo de LIT descargado en tal lector. Son describen plenamente lectores a modo de ejemplo en el documento con n.º de expediente del mandatario MSFT-

0123, presentado de forma simultánea con el presente documento.

El cliente de canalización de cumplimiento 86 es preferiblemente un cliente independiente de Cola de Mensajes de MICROSOFT® (MSMQ, *MICROSOFT® Message Queue*), la cual se encuentra disponible con la familia de productos de WINDOWS® 2000 Server. Este componente implementa la canalización de comunicación asíncrona entre la ISAPI de servidor de descarga 78 y la base de datos de cumplimiento 89. La ISAPI 78 registra cada transacción de descarga por medio de un mensaje que se publica en el cliente de MSMQ local 86 en cada servidor de contenido 76, el cual, a su vez, almacenará y reenviará tales mensajes en una forma flexible a un cliente de MSMQ 86 similar que está alojado en el servidor de cumplimiento 84. Esta canalización también se usará para invalidar entradas almacenadas en memoria caché en una memoria caché de RAM de ISAPI (que está ubicada en los servidores de contenido 76), por medio de unos mensajes que se publican desde el servidor de cumplimiento 84 en la DLL de ISAPI 78 por medio del mismo conjunto de clientes de MSMQ alojados de forma local.

Al igual que en la arquitectura de servidor 70, el almacén de contenido 80 de la arquitectura de servidor 70' es preferiblemente un sistema de gestión de bases de datos o sistema de archivos grande y unido a red. Este sirve como un repositorio para los títulos de LIT que son usados por la ISAPI de servidor de descarga 78 cuando se da cumplimiento a los pedidos. Este servidor preferiblemente ejecuta un Servidor Avanzado de WINDOWS® 2000 y expone una ruta de UNC a la que puede acceder la DLL de ISAPI de servidor de descarga. Eso se puede lograr por medio de una aplicación de configuración que es provista por DAS. También es preferible que el almacén de contenido 80 exista por detrás de un cortafuegos y no esté expuesto a la web.

El servidor de cumplimiento 84 es preferiblemente un Servidor Avanzado de WINDOWS 2000 que ejecuta SQL 7.0 de MICROSOFT® (o posterior). Este servidor aloja una base de datos de cumplimiento 89, una base de datos de registro 91, un cliente de canalización de cumplimiento 86 y un objeto de COM de canalización de cumplimiento 87. La base de datos de cumplimiento 84 aloja tablas que ponen en correspondencia la combinación de un "ID de libro" y "Tipo de ID de libro" con la ubicación física de cada archivo de LIT en el almacén de contenido 80. La base de datos 84 también contiene una información acerca de cada archivo de LIT que se puede requerir para el cumplimiento, tal como el título del libro, el autor del libro, el nivel de protección de DRM y / o el precio sugerido de comercio al por menor. El intervalo completo de información puede variar de acuerdo con las reglas / prácticas comerciales de cada centro de cumplimiento (por ejemplo, la entidad que opera el servidor de contenido 76), pero preferiblemente la información incluye aquellos artículos que se han enumerado en lo que antecede. Se puede proporcionar una secuencia de comandos de línea de comandos que crea las tablas y los procedimientos almacenados necesarios para esta base de datos, además de añadir entradas de muestra que pueden ser usadas como referencia por el centro de cumplimiento cuando se diseñan sus procedimientos de gestión de contenidos.

La base de datos de registro 91 se usa para registrar cada transacción de descarga a partir de la DLL de ISAPI de servidor de descarga 78 (para la facturación / notificación posterior cuando sea aplicable). El cliente de canalización de cumplimiento 86 es preferiblemente un cliente independiente de Cola de Mensajes de MICROSOFT® (MSMQ, *MICROSOFT® Message Queue*) el cual existe en los servidores de contenido / descarga 76, tal como se ha descrito en lo que antecede. El objeto de canalización de cumplimiento 87 es preferiblemente un objeto de COM que es desencadenado por el cliente independiente de MSMQ que está alojado en el servidor de cumplimiento 84 cada vez se escribe un mensaje entrante en la cola de llegada en este servidor. El objeto de canalización de cumplimiento 87 extrae la información de registro de cada mensaje de MSMQ y la escribe en la base de datos de registro 91, en donde esta se puede usar más adelante mediante la notificación de secuencias de comandos. Adicionalmente, el objeto de canalización de cumplimiento 87 será desencadenado por cambios en la base de datos de cumplimiento 89 e insertará cualquier información de actualización / eliminación en los diversos clientes independientes de MSMQ 86 que están alojados en los servidores de descarga 76.

La herramienta de gestión de contenidos 82 es responsable de la gestión de la información que está almacenada en la base de datos de cumplimiento 89. Cuando se añaden archivos de LIT al almacén de contenido 80, esta herramienta escribe los campos apropiados en la base de datos de cumplimiento 89 (por ejemplo, la puesta en correspondencia de ID de libro con unas ubicaciones físicas) de tal modo que el módulo de complemento de almacén de contenido 88 pueda hallar más adelante los archivos de LIT solicitados. De forma similar, si se hacen cualesquiera cambios (por ejemplo, un cambio en el nivel de DRM en un archivo de LIT) esta herramienta proporciona la interfaz a partir de la cual los responsables de la función de gestión de contenidos dentro del centro de cumplimiento (es decir, administradores humanos de contenido) llevarían a cabo estas tareas.

Los centros de cumplimiento 73 pueden lograr la tarea de gestión de contenidos mediante la construcción de un conjunto de páginas ASP que, por medio de objetos de COM de IIS convencionales, escriben la totalidad de la información relevante en la base de datos de cumplimiento 89 y colocan el archivo de LIT entrante (ya cifrado como una copia sellada por la fuente) en un servidor de almacenamiento provisional 83, el cual imitaría la estructura de directorios del almacén de contenido de producción 80. A partir de ahí, los archivos de LIT se replicarían de forma automática usando, por ejemplo, el Servidor de Replicación de Contenido de Servidor de Sitio 2000, en el servidor de almacén de contenido de producción. No necesariamente se requiere el servidor de almacenamiento provisional 83 para implementar el sistema de DAS, pero es un enfoque ventajoso replicar los archivos de LIT a partir de la red del socio de cumplimiento en los servidores de almacén de contenido de producción mediante el uso de herramientas tales como un servidor de replicación de contenido de MICROSOFT® (CRS, *content replication*

server).

Los servidores de activación 94 realizan la función de proveer cada lector de cliente (por ejemplo, el lector de PC 90 o el dispositivo de lectura dedicado 92) con un repositorio seguro único y un certificado de activación. Un repositorio seguro a modo de ejemplo, y sistemas y procedimientos para proporcionar el mismo, se divulgan en el documento con n.º de expediente del mandatario MSFT-0126, presentado de forma simultánea con el presente documento.

El repositorio seguro y el certificado de activación asocia el lector activado con un rol en línea (por ejemplo, un ID de PASSPORT™ de MICROSOFT®) para asegurar que los usuarios sean capaces de leer sus títulos adquiridos de forma legítima en todas las instancias de lectores que son propiedad de estos o que han activado para su rol (pero no en lectores no activados, o lectores no activados para ese rol) - suponiendo que estos activen sus lectores usando la misma contraseña e ID de usuario cada vez.

El servidor de activación 94 incluye un objeto de PASSPORT 96 y una DLL de extensión de ISAPI de servidor de activación 98. El objeto de PASSPORT 96 proporciona las interfaces requeridas en los servidores de PASSPORT™ que autentican a los usuarios finales usando, por ejemplo, sus cuentas de Hotmail (u otras credenciales de PASSPORT). De acuerdo con unos aspectos de la presente invención, el presente objeto asocia de forma ventajosa el certificado de activación con un rol, en lugar de un único PC, permitiendo de este modo que cada rol utilice múltiples lectores para leer títulos de nivel 5. A pesar de que se apreciará que unir los títulos de nivel 5 a un "rol" permite un uso más amplio de los títulos de nivel 5 que si estos se hubieran enlazado a un único dispositivo, definiendo un rol en términos de una autoridad de espacio de nombres establecida tal como lo son los servidores de PASSPORT también sirve al fin de limitar el uso no restringido de los títulos de nivel 5 que, de lo contrario, podría existir si se permitiera que los usuarios usaran una marca arbitraria para funcionar como un rol. En el caso de las credenciales de PASSPORT, la información personal en relación con un usuario particular está asociada con las credenciales de PASSPORT de ese usuario, posiblemente variando de la cuenta de correo electrónico del usuario a su número de tarjeta de crédito. Por lo tanto, es poco probable que un usuario comparta su ID y contraseña de PASSPORT con un gran grupo de personas, asegurando de ese modo que el rol para el cual se activa un lector está asociado genuinamente con un usuario particular (o, posiblemente, una familia que comparte una única cuenta de PASSPORT). A pesar de que un servidor de PASSPORT es una autoridad de espacio de nombres a modo de ejemplo que puede proporcionar esta característica ventajosa, se apreciará que se podrían usar otras autoridades de espacio de nombres sin apartarse del ámbito de la invención. En una realización alternativa de este tipo, el objeto de PASSPORT 96 se sustituiría con un objeto diferente el cual se comunica con la autoridad de espacio de nombres alternativa.

La DLL de extensión de ISAPI de servidor de activación 98 lleva a cabo unas tareas que están asociadas con el procedimiento de activación en los servidores de activación de extremo de cliente, incluyendo recibir un ID de soporte físico que es subido por el cliente de lector, crear un ID de máquina único en base al ID de soporte físico, publicar una solicitud en el servidor o servidores de repositorio seguro 100, firmar cada repositorio seguro único que se recibe del servidor o servidores de repositorio seguro 100, generar y (opcionalmente) cifrar el certificado de activación, actualizar la base de datos de activación 102 y descargar tanto el repositorio seguro como el certificado de activación, en el cliente de lector. El procedimiento de activación se describe más en concreto en lo sucesivo en conexión con la figura 8.

Los servidores de repositorio seguro 100 son preferiblemente servidores autónomos que están ubicados por detrás de un cortafuegos en un centro de datos. Los servidores de activación 94 acceden a estos para generar unos repositorios seguros individualizados para cada lector que se esté activando. Estos servidores son preferiblemente dedicados, y preferiblemente ejecutan un servicio de WINDOWS® 2000 o de WINDOWS NT® que expone una interfaz de socket a los servidores de activación 94. El servicio de repositorio seguro enlaza con un ejecutable distinto para cada combinación única de ID de máquina y de ID de PASSPORT que sea publicada. La tarea de preparar un repositorio seguro individualizado es, en muchos casos, intensiva desde el punto de vista del cómputo. Por lo tanto, en una realización preferida, hay un número suficiente de servidores de repositorio seguro 100 para proporcionar unos repositorios seguros a lectores en tiempo real (por ejemplo, unos pocos segundos por activación), teniendo en cuenta el volumen esperado de tráfico de activación.

La base de datos de activación 102 es preferiblemente un servidor basado en SQL 7.0 de MICROSOFT® que almacena una información de activación en relación con cada usuario final del lector 90 o 92 (en base a sus ID de PASSPORT™). Tal información puede incluir: ID de máquina, el número de lectores activados, la fecha de la primera activación, el ID de producto (PID, *product ID*) para cada una de las instalaciones de lector, su información de perfil de PASSPORT™, etc. Esta información se usa para garantizar que los usuarios no están abusando del sistema, ayudando a los usuarios a recuperarse de bloqueos de la unidad de disco duro, y ayudando a permitir a los usuarios a continuar leyendo el contenido que compraron los mismos después de una actualización de soporte físico. Por ejemplo, el número de lectores activados y la fecha de la primera activación que está asociada con una credencial de PASSPORT particular se podrían usar para imponer un límite sobre el número de activaciones (por ejemplo, no más de cinco activaciones para un rol dado en los primeros 90 días a continuación de la primera activación, con una activación adicional permitida cada 90 días a continuación de lo anterior, hasta un total de 10 activaciones). Imponer un límite de este tipo (o algún otro tipo de límite) tiene el efecto de evitar la proliferación no controlada de lectores que están activados para un único rol (lo cual, en el peor caso, podría dar como resultado un

título de nivel 5 que es legible en millones de dispositivos de lectura, frustrando de ese modo el fin de controlar la distribución de contenido valioso). Adicionalmente, la otra información en la base de datos de activación 102 posibilita que los usuarios usen títulos de nivel 5 después de una actualización de soporte físico (o después de un bloqueo del disco duro), sin tener que volver a descargar títulos o licencias. En esta instancia, todo lo que es necesario que haga un usuario activar el lector sobre el soporte físico actualizado (o reparado) con el mismo ID de PASSPORT™.

El servidor de base de datos de activación 102 está ubicado preferiblemente por detrás de un cortafuegos y solo pueden acceder al mismo los servidores de IIS de activación de extremo de cliente en la misma red privada en la que están ubicados los servidores de repositorio seguro. Se puede acceder a una réplica de la base de datos de activación 102 por medio de secuencias de comandos fuera de línea para generar notificaciones del número de activaciones por día, semana, mes, promedio de activaciones por ID de PASSPORT™, etc.

Infraestructura de recibo

Tal como se ha descrito brevemente en lo que antecede, la arquitectura de servidor de la presente invención incluye un objeto de cifrado de URL 74, el cual cifra determinados parámetros en relación con la venta de un libro electrónico 10, en donde los parámetros cifrados se pueden incluir en un URL. Lo siguiente es una visión de conjunto más detallada del uso del objeto de cifrado de URL 74.

El objeto de cifrado de URL 74 facilita un desacoplamiento del vendedor de libros electrónicos (por ejemplo, el comerciante minorista) con respecto a la entidad que proporciona en realidad el archivo de LIT al comprador (por ejemplo, un centro de cumplimiento). El objeto de cifrado de URL 74 realiza esta función mediante el cifrado de una información en relación con el libro electrónico comprado con un secreto (por ejemplo, la clave simétrica 75), el cual se comparte entre el centro de cumplimiento y el comerciante minorista. En un escenario a modo de ejemplo, el comerciante minorista entabla una relación comercial (por ejemplo, un contrato) con un centro de cumplimiento, mediante lo cual el centro de cumplimiento acuerda proporcionar servicios de descarga para el comerciante minorista que no tiene en realidad unas existencias electrónicas de libros electrónicos o los dispositivos de servidor necesarios para descargar libros electrónicos a un gran número de compradores. Como parte de esta relación, el comerciante minorista y el centro de cumplimiento acuerdan una clave simétrica secreta 75, la cual será usada por el objeto de cifrado de URL 74 en el sitio de comerciante minorista, y por la DLL de extensión de ISAPI 78 en el sitio de centro de cumplimiento. En esencia, el comerciante minorista usa el objeto de cifrado de URL 74 y la clave simétrica secreta 74 para cifrar una información en relación con la compra de un libro electrónico, e incluye esta información cifrada como un parámetro para un URL que señala el sitio de centro de cumplimiento. El URL se presenta entonces en el soporte lógico de navegación del comprador como una "página de recibo", en donde el "recibo" es un hipervínculo al URL que invoca la descarga a partir del centro de cumplimiento. Cuando el usuario sigue el vínculo, el centro de cumplimiento recibe el parámetro cifrado y lo descifra usando la clave simétrica 75 de secreto compartido. Debido a que el parámetro está cifrado, cualquier información secreta que sea necesario intercambiar entre el comerciante minorista y el sitio de cumplimiento se puede proporcionar de forma segura de forma cifrada al sitio del comprador, debido a que el comprador no conoce la clave simétrica 75 (y, presumiblemente, otros ajos al acecho en la web tampoco tienen acceso a la clave simétrica 75). Además, cuando el centro de cumplimiento descifra la información cifrada para obtener la información necesaria para la descarga, el descifrado apropiado de la información autentica el "recibo" como generado por un comerciante minorista legítimo, debido a que presumiblemente nadie que no sea el comerciante minorista tiene la clave simétrica 75 necesaria para crear de forma apropiada el parámetro cifrado. Se debería hacer notar que la clave simétrica 75 es meramente a modo de ejemplo del tipo de secreto que se podría compartir entre un comerciante minorista y un centro de cumplimiento para permitir esta forma de comunicación. En una realización alternativa, se podrían usar unos pares de claves asimétricas, o el comerciante minorista y el centro de cumplimiento podrían acordar un procedimiento de cifrado sin claves secreto.

La figura 5 muestra el uso del objeto de cifrado de URL 74 para crear el parámetro cifrado. El objeto de cifrado de URL 74 cifra el parámetro de URL usando una clave simétrica 75 (el "secreto" de URL) que se comparte entre la ISAPI de servidor de descarga 78 y el objeto de cifrado de URL 74 en el servidor de comercio al por menor. En un escenario alojado, en el que un centro de cumplimiento prevé la descarga de archivos de LIT vendidos por un gran número de sitios de comercio al por menor, se proporciona una clave simétrica 75 a cada comerciante minorista cuando estos celebran un contrato con el centro de cumplimiento 73. Es importante hacer notar que esta clave simétrica 75 puede ser única para cada comerciante minorista 71. El centro de cumplimiento 73 puede almacenar las claves para cada comerciante minorista en la base de datos de cumplimiento 89. Se debería hacer notar que la clave simétrica 75 que se usa para el cifrado del parámetro de URL es diferente de las claves simétricas 14A que son generadas por la herramienta de gestión y de cifrado de contenidos 82 para cifrar los archivos de LIT.

Un procedimiento exportado único sobre el objeto de cifrado de URL 74 ("Encrypt()"), crea los parámetros de URL cifrados. Preferiblemente, el procedimiento de Encrypt() toma los siguientes parámetros para que sean incorporados en el blob cifrado que se usará en el URL:

TransactionID - una cadena que identifica de forma única cada transacción en el sitio de librería 72;
BookID - un identificador único, el cual es usado por el servidor de descarga 76 para localizar el archivo de LIT

apropiado por medio del módulo de complemento de almacén de contenido 88 (el cual consulta el BookID en la base de datos de cumplimiento 84);
BookIDType - identifica de qué tipo es el ID (por ejemplo ISBN, DOI, PATH, etc.). El objeto de cifrado de URL 74 preferiblemente no valida este campo, o su relación con el ID. La ISAPI de servidor de descarga 78 usa más adelante este campo como un parámetro de entrada adicional en la consulta realizada por el módulo de complemento de almacén de contenido 88;
UserName - una cadena que contiene el nombre del propietario legítimo del libro electrónico comprado. Esta cadena preferiblemente establece una correspondencia con el consumidor que se enumera en la tarjeta de crédito que se usa para la transacción comercial, a pesar de que esto se deja como política a ser establecida por la fuente de contenido (por ejemplo el editor) de acuerdo con el centro de cumplimiento. Esta cadena es el nombre que será usado posteriormente por la ISAPI de servidor de descarga 78 para sellar de forma individual los títulos (es decir, para generar el exlibris). Se recordará que los títulos individualizados (por ejemplo, el nivel 3 y el nivel 5) incorporan el nombre del usuario en el archivo de LIT y enlazan ese nombre a la clave de descifrado, de tal modo que se pueda detectar el origen de la distribución no autorizada de contenido. Por lo tanto, es preferible que el nombre del comprador provenga de una fuente fiable (tal como la tarjeta de crédito del usuario), en lugar de provenir de una fuente no verificable (tal como una entrada de usuario). A pesar de que el ejemplo anterior supone que se insertará un nombre en este campo, los contenidos reales del campo son determinados por el comerciante minorista, y estos podrían contener cualquier información (por ejemplo, número de tarjeta de crédito, ID de transacción, ID de recibo, etc.) - preferiblemente una información que se refiere a la compra o al comprador con el fin de permitir la vigilancia y el seguimiento de la copia;
ID de PASSPORT - El ID de rol que está asociado con el usuario, el cual es provisto por el usuario durante la activación. Este campo es usado posteriormente por el servidor de contenido para una comparación con el ID de activación en el certificado de activación. Se debería hacer notar que, a pesar de que el ID de PASSPORT está contenido en el certificado de activación, ese ID no es subido al servidor de librería 72 durante la transacción de compra. En su lugar, el procedimiento de activación, además de insertar el ID de PASSPORT en el certificado de activación, también almacena el ID de PASSPORT en el registro en el dispositivo informático del usuario, y este es la instancia de registro del ID de PASSPORT que se proporciona al servidor de librería 72; y
SecurityLevel - esta cadena indica qué nivel de DRM requiere esta publicación particular. Esta se convertirá posteriormente en un número y será marcada en los metadatos del título 12 por la ISAPI de servidor de descarga 78;

Opcionalmente, los siguientes parámetros de entrada también se pueden incluir con una solicitud:

Coste - el precio que el comerciante (es decir, el comerciante minorista 71) pagó por ese título de libro electrónico en el momento en el que se vendió el título al consumidor;
MSRP - precio recomendado por el editor en el momento en el que se vendió el título;
Precio - el precio por el cual se vendió el título de libro electrónico. Este es un parámetro opcional, y de estar presente será usado por el servidor de descarga para fines de registro y, en potencia, para fines de facturación;
FriendlyFileName - esta cadena es usada por el servidor de descarga cuando se establece el nombre de archivo para el archivo de LIT que se está descargando por medio del encabezado de HTTP de respuesta; y
CustomerID - un identificador único para el usuario final que compra el título de libro electrónico. El comerciante (es decir, el comerciante minorista 71) puede requerir esta información como parte de las notificaciones que este recibe del centro de cumplimiento.

La lista de parámetros anterior es extensible y no se debería interpretar como limitante del conjunto completo que es soportado por el objeto de cifrado de URL 74. Se pueden añadir pares de atributo - valor adicionales, debido a que el objeto de cifrado de URL 74 cifrará la totalidad del conjunto de valores que se pasan y los devuelve a la función que llama.

Preferiblemente, el objeto de cifrado de URL 74 añade una marca de tiempo y una versión. La marca de tiempo es una cadena que preferiblemente contiene una representación del número de nanosegundos que han pasado desde 1601 (en tiempo de sistema GMT) en la máquina local en la que se instala el objeto de cifrado de URL 74. Este valor puede ser usado por el servidor de descarga para calcular un tiempo de vida (TTL, *time-to-live*) con el fin de evitar los ataques de reproducción (es decir, el robo por parte de una persona de un URL y su reproducción para descargar un libro. El campo de versión es una cadena no cifrada que identifica la versión del objeto de cifrado de URL 74 que creó el blob cifrado en el URL.

Después de que el comerciante minorista 71 haya obtenido la cadena cifrada del objeto de cifrado de URL 74, el comerciante minorista 71 construye una solicitud de POST que señala el servidor de descarga 76 para el cumplimiento. El blob cifrado que es devuelto por el objeto de cifrado de URL 74 está incluido en el cuerpo de cada POST. Además de los parámetros cifrados, los comerciantes minoristas pueden necesitar proporcionar un ID de comerciante minorista en el URL el cual identifica al comerciante minorista. Esto puede ser usado por la DLL de ISAPI de servidor de descarga 78 para poner en correspondencia la solicitud entrante con la clave simétrica de URL 75 apropiada para el descifrado en el caso en el que múltiples comerciantes minoristas están siendo soportados por un sitio de servidor de descarga único 76. Este es un campo opcional y si, en el caso de no proporcionarse, la DLL de ISAPI de servidor de descarga 78 en el sitio de cumplimiento 73 usará más adelante su clave simétrica por defecto 75 provista durante la configuración para descifrar los URL.

Por lo tanto, de acuerdo con lo anterior, suponiendo una entrada al objeto de cifrado de URL 74 tal como:

TransactionId=R6RAKHAL9TS12JTG00QP9ESTQ4&BookId=044021145X&BookIdType=ISBN&Username=Pavel+Zeman&SecurityLevel=3

El objeto de COM de cifrado 74 puede devolver el siguiente blob cifrado: LCfsQCLuMg9UZtWxIdYTfw%2BzMtjXAN%2BiU0YHaomrY3ydXhw3p9T1wZuH%2BFEHTEP687Nq17wbMMwnbtHAkIjkKhKS%2BYKwgHj7%2FNr%2BvBD50APwqMbvN3saNBrPxG8s1ziU1iX%2F%2BSS%2FttA%2F4GZjRMo5uXWM%2BZr5dYHk SfWfBBC0iH7uLFo1yIz8LSI=&Version=1.0

El URL del objeto de cifrado de URL 74 codifica el blob cifrado, de tal modo que este cumple con la norma de HTTP requerida para los URL en ANSI. El objeto de cifrado de URL 74 acepta cadenas tanto de Unicode como de UTF-8, y maneja la conversión de UTF-8 a partir de Unicode de forma interna. Opcionalmente, el objeto de cifrado de URL 74 usa UTF-8, si se proporciona, lo cual reduce el tamaño del blob de extremo cifrado que ha escapado resultante para una entrada no Unicode a aproximadamente la mitad. El objeto de cifrado de URL 74 preferiblemente computa una función criptográfica de troceo de los datos que se van a cifrar antes de cifrar tales datos, e incluye la función de troceo con (por ejemplo, delante de) los datos cifrados y codificados. Esta función de troceo se puede usar más adelante para una comparación por el servidor de descarga para verificar que los datos descifrados no se han sometido a manipulación indebida entre el sitio de comercio al por menor y el servidor de descarga. Por ejemplo, el parámetro completo (por ejemplo, que se va a incluir en el cuerpo de una solicitud de POST), puede indicar:

VALUE="&Hash=bCt/xn4lfTJw7cPQjstge+6Lifc=&Data=zAybPKWl23d2O+...encoded_data_continues...MSSD8Eyw==&Version=1.5"

La ISAPI de servidor de descarga 78 es responsable de la individualización y la descarga de títulos de libros electrónicos en los usuarios finales. Asimismo, el análisis sintáctico y la validación de cada URL que es generado por el objeto de cifrado de URL 74 es realizado por la DLL de ISAPI de servidor de descarga 78. Esto incluye descifrar el URL usando la clave simétrica 75 apropiada, la cual puede ser o bien una clave por defecto o bien, en el caso en el que se proporciona un ID de comerciante minorista, una cadena que resulta de una consulta de base de datos por medio del módulo de complemento de almacén de contenido. La DLL de ISAPI de servidor de descarga 78 también resuelve la puesta en correspondencia del ID de libro y el tipo de ID de libro a partir del URL pasado para dar una ubicación de compartición de archivos preferiblemente por medio de un módulo de complemento. El módulo de complemento recupera esa información de la base de datos de cumplimiento y posibilita que los proveedores de contenido añadan sus propias reglas de convención de nomenclatura y base de datos de puesta en correspondencia.

La ISAPI de servidor de descarga 78 también determina el nivel de protección de DRM que se requiere para la descarga del archivo de LIT solicitado. El nivel se determinará en base a una indicación a partir de la base de datos de cumplimiento 89 del nivel de DRM para el título que se está descargando. Por ejemplo, si el URL que es creado por el comerciante minorista define un nivel de DRM más bajo que el que se especifica en la base de datos de cumplimiento, se devolverá un mensaje de error al comerciante minorista 71. Asimismo, la ISAPI capturará el título de libro electrónico para la descarga a partir del almacén de contenido 80 en una memoria caché local, si no está almacenada en memoria caché, despojará la clave simétrica 14A (véase la figura 1) del archivo de LIT antes de su almacenamiento en memoria caché de forma local en el servidor IIS, y almacenará en memoria caché la clave 14A en memoria para su uso futuro.

En el caso de los títulos de nivel 3 de DRM, la ISAPI de servidor de descarga 78 inserta el nombre del usuario a partir del blob con cifrado de URL en el archivo de LIT como una secuencia separada, vuelve a aplicar una función de troceo a los metadatos con los contenidos de esta nueva secuencia, sella la clave simétrica 14A con la función criptográfica de troceo recién computada, y vuelve a insertar la clave simétrica recién sellada en el archivo de LIT para la descarga. En el caso de los títulos de nivel 5 de DRM, la ISAPI de servidor de descarga genera una estructura de XML de licencia (además de las acciones de nivel 3 que se han hecho notar en lo que antecede), sella la clave simétrica con la clave pública procedente del certificado de activación del usuario final, e incrusta la licencia en el archivo de LIT.

La ISAPI de servidor de descarga 78 también descarga el archivo de LIT en el usuario final, libera el almacenamiento temporal que se usa durante la individualización del archivo de LIT, y registra cada solicitud de descarga o bien en un archivo local en el servidor IIS o bien en la base de datos de registro 91, por medio de la canalización de cumplimiento asíncrona que se analiza en lo sucesivo. Esto se puede realizar por medio de una publicación de mensaje en el cliente de MSMQ local que reside en cada servidor de descarga 76.

La DLL de extensión de ISAPI de servidor de descarga 78 responde a un conjunto de comandos definidos por el parámetro "?action=". Preferiblemente, hay dos acciones que son soportadas por la ISAPI de servidor de descarga 78: descarga y verificación. La acción de descarga es el comando que da lugar a que la ISAPI 78 siga las etapas

que se identifican en la figura 7 y devuelva un título de libro electrónico al usuario. La acción de verificación se usa para solicitar a la ISAPI 78 que verifique que un BookID dado existe en el almacén de contenido 80 y está listo para la descarga. El comando (descarga) más común se puede parecer al siguiente URL: http://contentprovider.com/isapi/ds.dll?action=download&value=...

El parámetro /isapi/ en el URL indica la raíz virtual en la que se instaló la ISAPI 78. En el presente ejemplo la ISAPI 78 se denomina ds.dll (DLL de servidor de descarga). El nombre de la ISAPI 78 es seguido por la acción, la cual es seguida por los parámetros relevantes para llevar a cabo esa acción (el parámetro de "valor" en el ejemplo anterior). En el presente ejemplo, los parámetros relevantes comprenden el blob cifrado que es generado por el objeto de COM de cifrado de URL 74.

Cada solicitud de descarga incluirá, en el cuerpo del POST, el URL para la página de manejo de errores en el sitio de comerciante minorista 71. El servidor de descarga 76 usa este URL siempre que tiene lugar un error y redirige al cliente hacia esa página, con el código de error etiquetado en la cadena de consulta. En el caso de un error, los comerciantes minoristas pueden proporcionar un UI de HTML, un número de soporte, un vínculo de correo electrónico, o instrucciones de resolución de problemas. De acuerdo con un aspecto de la presente invención, la DLL de ISAPI de servidor de descarga 78 preferiblemente no da errores, sino que más bien, redirige a los usuarios hacia el URL de manejo de errores requerido a partir de la solicitud de POST.

Desde los puntos de vista de la operabilidad y de una gestión de centros de datos, la ISAPI 78 expondrá unos contadores de rendimiento (es decir, contadores de PerfMon) y eventos de WINDOWS NT®. Estas son unas prácticas operativas típicas de WINDOWS® 2000 y de WINDOWS NT® para la implementación de centros de datos y la gestión de componentes de servidor. Los eventos de WINDOWS® 2000 y de WINDOWS NT® se registran siempre que tiene lugar un error. Algunos de los eventos clave que preferiblemente son registrados por la ISAPI 78 son:

Fallo al Inicializar - cualquier ajuste de configuración y / o de entorno requerido ausente que diera lugar a que la ISAPI fallara durante la carga;
Fallo al conectar al almacén de contenido - o bien la ruta de UNC que es devuelta por el módulo de complemento de almacén de contenido era no válida o bien el almacén de contenido 80 y / o la ruta de red hasta este está caída. En uno u otro caso, la ISAPI ha de registrar un error de tal modo que los operadores de centros de datos pueden emprender una medida apropiada;
Solicitud de URL ilegal - este evento se ha de registrar siempre que una solicitud de URL no cumple con el formato esperado o no ha sido cifrada por la clave simétrica 75 compartida entre la ISAPI 78 y el objeto de COM de URL 74. Idealmente, se debería publicar el URL completo en el evento, junto con el IP de origen, para fines de auditoría;
Fallo al localizar un archivo de LIT - o bien la ruta en la solicitud era no válida o bien el archivo de LIT esta ausente de la cuota objetivo;
Fallo al almacenar en memoria caché el archivo de LIT – esto puede ocurrir si el servidor de contenido 76 que aloja la ISAPI 78 se queda sin memoria, o si un problema de red tuvo lugar durante la transmisión de archivos desde el almacén de contenido 80;
Fallo al crear un exlibris - este evento se ha de registrar en cualquier momento en el que la ISAPI 78 sea incapaz de llevar a cabo el sellado individual del título. La naturaleza del error se ha de incluir en el propio evento, para la posterior depuración de errores;
Fallo al descargar un título - este evento se ha de registrar siempre que falla una descarga (tiempo de expiración, conexión interrumpida, etc.); y
Eventos de Inicio / Apagado - siempre que se (des)carga la ISAPI 78, esta ha de registrar un evento informativo a esta extensión, de tal modo que exista una visibilidad apropiada. Puede haber casos en los que una ISAPI 78 se descarga mediante IIS y los operadores de centros de datos necesitan reiniciar el IIS o incluso WINDOWS NT® para llevar el servidor de contenido 76 de vuelta a un estado completamente operativo.

La ISAPI de servidor de descarga 78 también preferiblemente expone los siguientes contadores de rendimiento:

Solicitudes de descarga totales - medidas en solicitudes únicas aceptadas desde el último inicio del servidor;
Descargas con éxito totales - medidas en solicitudes únicas a las que se da cumplimiento desde el último inicio del servidor;
Solicitudes de descarga / s - número de solicitudes entrantes únicas / s;
Descargas con éxito / s - medidas en solicitudes únicas a las que se da cumplimiento por segundo;
Solicitudes de descarga pendientes - número total de solicitudes que se están procesando en cualquier momento dado;
Solicitudes de descarga fallidas - número total de fallos desde el último inicio del servidor;
Tiempo de procesamiento de solicitud promedio - medido en milisegundos, este refleja el tiempo promedio que está llevando a la ISAPI el procesamiento de las solicitudes entrantes; y
Tiempo de procesamiento de última solicitud - medido en milisegundos, este refleja el tiempo que llevó a la ISAPI el procesamiento de su solicitud más reciente;
Combinados, los eventos de WINDOWS NT® y los contadores de PerfMon permitirán que un hospedador de los conjuntos de aplicaciones de gestión y de supervisión de centros de datos existentes administre la ISAPI 78

durante la implementación del sistema.

Canalización de cumplimiento asíncrona

La canalización de cumplimiento asíncrona realiza el registro asíncrono de solicitudes de descarga en la base de datos de registro 91 e invalidaciones asíncronas de entradas almacenadas en memoria caché por la DLL de ISAPI de servidor de descarga. El servidor de canalización de cumplimiento asíncrona logra estas tareas al sacar partido de la funcionalidad existente de almacenar - y - reenviar que es provista por el componente de Cola de Mensajes de MICROSOFT® (MSMQ, *MICROSOFT® Message Queue*) de Windows® 2000.

La arquitectura para la canalización de cumplimiento se muestra en las figuras 4 y 6. El objeto de canalización de cumplimiento 87 es ejecutado por el servicio de desencadenamiento de MSMQ y escribe en la base de datos de registro cada vez que aparece un mensaje entrante en la cola de llegada del cliente de MSMQ local 86. Preferiblemente, el objeto de canalización de cumplimiento 87 se implementa como un objeto de COM. El agente de actualización de memoria caché 85 tiene un ejecutable asociado que es engendrado por un desencadenador de SQL en cualquier momento en el que una actualización o una operación de eliminación tenga lugar en la base de datos de cumplimiento 89. La DLL de extensión de ISAPI de servidor de descarga 78 tanto leerá como escribirá en / del cliente independiente de MSMQ local 86.

Una función de registro preferiblemente se ejecuta en la base de datos de registro 91 para hacer persistir todos los parámetros que se pasan en el cuerpo de cada solicitud de POST de descargas. El objeto de COM de canalización de cumplimiento 87 se instancia en el servidor de cumplimiento 84 a medida que cada mensaje de registro individual llega a la cola de llegada del cliente independiente de MSMQ local 86 en el servidor de cumplimiento 84. El esquema de la base de datos de registro 91 se describe en detalle adicional en lo sucesivo. La información procedente del cuerpo de cada solicitud de POST a los servidores de descarga 76 se convierte en un formato de mensaje de MSMQ y se publica en la cola de llegada del cliente de MSMQ local 86 en el servidor de cumplimiento 84.

Entonces, el cliente de MSMQ 86 en el servidor de cumplimiento 76 recoge este paquete de mensajes e invoca, por medio del servicio de desencadenamiento de MSMQ, el objeto de COM de canalización de cumplimiento 87, el cual convierte el mensaje a un formato de base de datos y lo escribe en la base de datos, por medio de un Nombre de Fuente de Datos (DSN, *Data Source Name*) en el servidor de cumplimiento 84 que abstrae el nombre, la ubicación y las credenciales de inicio de sesión para la base de datos de registro a partir del objeto de COM.

A medida que la herramienta de gestión de contenidos 82 actualiza y / o elimina anotaciones de la base de datos de cumplimiento 89, un ejecutable de agente de actualización de memoria caché 85 es desencadenado por el servidor de SQL (usando desencadenadores de eliminación / actualización de SQL convencionales). El agente de actualización de memoria caché 85 realiza una función similar a la del objeto de COM de canalización de cumplimiento 87, pero en el sentido opuesto. Dado que las operaciones de actualización y de eliminación en la base de datos de cumplimiento 89 pueden requerir actualizaciones de memoria caché para los DLL de ISAPI de servidor de descarga de extremo de cliente 78, este agente formará un mensaje de MSMQ y publicará este a través del cliente de MSMQ independiente 86 en la totalidad de los servidores de descarga 76 (el servidor de cumplimiento 84 debería tener una lista de todos los servidores de descarga 76 instalados).

Al recibir el mensaje de actualización de memoria caché, el cliente de MSMQ 86 en el servidor de descarga 76 llama a una función en la DLL de extensión de ISAPI 78 para actualizar la memoria caché. Esta acción elimina la entrada de memoria caché. La siguiente vez que se reciba una solicitud de este ID de libro particular, el servidor de descarga 76 consultará de nuevo la base de datos de cumplimiento 84 y, entonces, actualizará la memoria caché con el nuevo archivo de LIT y sus atributos relevantes. El tamaño de la memoria caché para el servidor de descarga 76 es determinado por la cantidad de memoria libre en el servidor físico. Es preferible que la DLL de ISAPI 78 atribuya hasta un 80 % de la memoria disponible en el servidor.

Generación de licencia

Se generan licencias preferiblemente para todos los títulos firmados y completamente individualizados (es decir, el nivel 5). La publicación de fuente también se puede ver acompañada por una licencia que constituye la firma de fuente, asegurando de este modo la autenticidad del libro electrónico que está siendo comprado por el consumidor. Las licencias se pueden delegar y la cadena de licencia preferiblemente se origina en los proveedores de publicaciones (es decir, autores y editores) y finaliza en el consumidor que realiza la compra. De acuerdo con la presente invención, preferiblemente los derechos pueden ser delegados por los emisores de licencia pero no por los consumidores. Una licencia de usuario final se genera por lo general en el momento de la descarga. En algunos casos, el comerciante minorista nombrará el propietario legítimo del libro electrónico (en el caso de sellar de forma individual) en la licencia, la cual se expone posteriormente por medio del UI (mediante una característica del lector 90 o 92) cuando los consumidores abren sus libros electrónicos.

Haciendo referencia a continuación a las figuras 4 y 7, en ellas se ilustra el flujo de procedimiento del procedimiento de generación de licencia. En la etapa 110, el procedimiento comienza y la solicitud (por ejemplo, la solicitud que se materializa en el blob de URL cifrado) se analiza sintácticamente en busca de atributos (la etapa 112). Si la solicitud se forma bien en la etapa 114, entonces se determina si la solicitud es para una licencia de nivel 5 (la etapa 118). En

caso negativo, entonces en la etapa 116, se devuelve un error y se detiene el procedimiento.

Si en la etapa 118 se determina que la solicitud es para una licencia de nivel 5, entonces se determina en la etapa 120 si se proporcionaron los principios de usuario. Si se proporcionaron estos, entonces los principios se hacen persistir en una base de datos local en la etapa 130. En caso negativo, entonces en la etapa 122, se determina si los principios de usuario se pueden recuperar de una base de datos local. En caso negativo, entonces estos se capturan del servidor de registro en la etapa 124, y si tienen éxito (la etapa 126), los datos se hacen persistir en la base de datos local en la etapa 130. Si la solicitud de capturar los datos del servidor de registro falló en la etapa 126, entonces se registra un evento (la etapa 128) y el procedimiento finaliza en la etapa 146.

Si en la etapa 122, los principios de usuario se pueden recuperar de la base de datos local, entonces el procesamiento continúa en la etapa 132, en la que la clave simétrica se cifra con la clave pública del usuario procedente del certificado. La etapa 132 también se realiza después de que los principios de usuario se hagan persistir en la base de datos local en la etapa 130. Entonces, el procesamiento avanza hasta la etapa 134, en la que se determina si la licencia está individualizada. La etapa 134 también es el la que el procesamiento continúa si en la etapa 118 se determina que la solicitud no es para una licencia de nivel 5.

Si en la etapa 134 la licencia está individualizada, el nombre del usuario se incluye en la licencia como el propietario legítimo. El procesamiento continúa en la etapa 136 en la que la estructura de XML de licencia se completa con el nombre del usuario y se firma. Si en la etapa 134, la licencia no está individualizada, entonces el procedimiento continúa en la etapa 138 en la que la estructura de XML de licencia se completa (sin el nombre del usuario) y se firma. En la etapa 140 se determina si tuvo éxito la generación de licencia. De ser así, entonces los contadores de rendimiento se actualizan y se devuelve el archivo de XML de licencia (la etapa 144) y, en caso negativo, se registra un evento y se devuelve un error (la etapa 142). Entonces, el procesamiento se completa en la etapa 146.

Una vez que se ha iniciado una descarga en el centro de cumplimiento 73 (es decir, los usuarios han realizado un pedido y, entonces, han pulsado sobre el vínculo a la descarga), en el caso de un título completamente individualizado la DLL de ISAPI de servidor de descarga 78 preferiblemente publica una solicitud en el módulo de concesión de licencia 77 para generar una licencia única para el título de libro electrónico que se está descargando. El URL de solicitud de descarga ha de proporcionar, como parte de los parámetros cifrados, una información de tal modo que el módulo de licencia puede sellar de forma individual cada licencia. Estos parámetros incluyen, para las copias de nivel 5, el certificado de activación cifrado que se descarga al usuario final durante la activación de su soporte lógico de lector. Un libro electrónico con licencia no se puede abrir a menos que la licencia requerida se encuentre presente y disponible para el lector.

Después de que los usuarios compren sus dispositivos de libro electrónico o descarguen el soporte lógico de lector 90, 92 de Internet, se alienta a estos a que activen sus lectores la primera vez que se lanza este (por ejemplo, inmediatamente después de la configuración para la aplicación de lector de ordenador portátil / ordenador de escritorio). La activación posibilita el soporte lógico de lector para la compra de copias completamente individualizadas y con protección de nivel 5. A continuación se describirá el flujo de procedimiento de la activación de lector, la experiencia del usuario final, y las interacciones de cliente - servidor que tienen lugar.

Cada vez que se lanza el lector 90 o 92, este comprueba si se ha activado. En caso negativo, el lector presentará un cuadro de diálogo que recuerda al usuario que este no será capaz de adquirir títulos con recargo que requieran una individualización plena para la distribución a menos que el usuario active el lector. Los usuarios pueden activar el lector desde cualquier sitio web de comercio al por menor, al tiempo que se compra con un navegador autónomo, o desde dentro de una característica de "librería integrada" del lector (el cual permite la comunicación con sitios de librería usando el propio soporte lógico de lector en lugar de un soporte lógico de navegación de propósito general). Lo que es más, el lector se puede activar desde dentro del sitio de un comerciante, al tiempo que se compra dentro de la característica de librería integrada del lector. Este escenario de activación puede tener lugar si, por ejemplo, el usuario rehusó activar el lector durante el primer lanzamiento y ahora desea comprar un título completamente individualizado (con protección de nivel 5), el cual requiere una activación.

Suponiendo que el usuario haya acordado activar el lector como en lo que antecede, el procedimiento que se da en lo sucesivo incluirá las siguientes etapas, tal como se ilustra con respecto a las figuras 4 y 8.

En la etapa 150, el cliente de lector se abre en la característica de librería integrada y conecta, por medio de capa de sockets segura (SSL, *secure sockets layer*), con los servidores de activación 94, en donde se pide a los usuarios de que inicien sesión usando, en el presente ejemplo, sus credenciales de PASSPORT™ (la etapa 152). Si el usuario no tiene una cuenta de PASSPORT™, se le proporcionará una en el vínculo para que se suscriba a la misma (la etapa 154). Es preferible que el URL para el servidor de activación 94 esté codificado de forma no modificable en un control de ActiveX de Activación usando una conexión de SSL de tal modo que el cliente puede garantizar que los servidores son en verdad los servidores de activación 94.

Una vez que se han autenticado las credenciales de PASSPORT™ del usuario (la etapa 156), una API de PASSPORT™ se consulta en busca del alias y la dirección de correo electrónico del usuario (la etapa 158). A continuación de lo anterior, en las etapas 160 - 162, los servidores de activación 94 solicitarán que el cliente (por

medio del control de ActiveX) descargue un ID de soporte físico único (por ejemplo, el cual, tal como se ha hecho notar en lo que antecede, se puede obtener a partir de componentes de soporte físico en el dispositivo informático del usuario los cuales identifican sustancialmente de forma única el dispositivo informático del usuario). A continuación, se determina en la etapa 164 si esta es una nueva activación para el lector (en contraposición a una "recuperación" de una activación anterior).

Si se determina que esta es una nueva activación en la etapa 164, entonces el procedimiento avanza hasta la etapa 168 para determinar si se ha alcanzado un límite de activación. Si se ha alcanzado el límite, entonces un mensaje de error se presenta en la etapa 172, incluyendo preferiblemente un número de teléfono de soporte. Entonces, el procedimiento finaliza en la etapa 198. De acuerdo con una característica de la presente invención, los usuarios pueden estar limitados en lo que respecta al número de activaciones que pueden realizar los mismos, y / o la tasa a la cual estos pueden realizar las mismas (es decir, cuántos lectores diferentes pueden activar estos para leer títulos de nivel 5 comprados con un rol dado). En el ejemplo de la figura 8, los usuarios se limitan a cinco activaciones dentro de un plazo de 90 días después de la primera activación del lector. Esto permite que los usuarios activen sus propios lectores, al tiempo que se previenen abusos del sistema de DAS. Un ejemplo del tipo de abuso que previene un límite de este tipo sería la compra por parte de un club de lectura de un libro electrónico con su cuenta de PASSPORT y permitir que miles de sus miembros activen sus lectores con las credenciales de PASSPORT del club de lectura. El límite a las activaciones también puede prever unas activaciones adicionales a medida que pasa el tiempo - por ejemplo, una activación adicional para cada periodo de 90 días después de los primeros 90 días, hasta un límite de 10 activaciones en total. Se apreciará que estos límites son meramente a modo de ejemplo, y se puede usar cualquier límite a las activaciones sin apartarse del ámbito de la invención.

Si el usuario no ha activado más de cinco lectores dentro de los primeros 90 días (o alcanzado un límite de activación aplicable diferente), una página de activación se presenta en el dispositivo del usuario (la etapa 170). Cuando el usuario devuelve el formulario, los servidores de activación determinar si el formulario ha sido completado (la etapa 174); si el formulario no ha sido completado, el procedimiento vuelve a la etapa 170 para volver a presentar el formulario hasta que el usuario completa el formulario. A continuación, en la etapa 176, se determina si esta activación es una recuperación. Si esta no es una recuperación, entonces se crea una nueva anotación para el usuario y lector y se incrementa el número de lectores que están activados para ese usuario (la etapa 180). Un par de claves de repositorio seguro previamente generado se recupera de una base de datos (la etapa 182) y también se generan unos certificados de activación (la etapa 184). Las claves de activación, el ID de usuario y el ID de máquina se hacen persistir en una base de datos en la etapa 186. En un ejemplo, a cada usuario (es decir, rol, tal como es identificado por, por ejemplo, una cuenta de PASSPORT) se le asigna un par de claves de activación el cual se usa en el certificado de activación para cada lector que active ese usuario, caso en el cual la clave simétrica 14A de los títulos de nivel 5 se cifra con la clave pública en el par de claves de activación en el momento en el que es preparado el título para ese usuario por el sitio de cumplimiento 73. En un perfeccionamiento adicional de ese ejemplo, cada dispositivo de lectura está equipado con un repositorio seguro individualizado y único que tiene un par de claves único asociado con el mismo, en donde el certificado de activación para un dispositivo dado contiene su clave privada en una forma que está cifrada por la clave pública que está asociada con el repositorio seguro. De esta forma, con el fin de presentar un título de nivel 5, es necesario que tanto el repositorio seguro como el certificado de activación se encuentren presentes, debido a que el repositorio seguro usa su clave privada para descifrar la clave privada del certificado de activación, la cual, a su vez, se usa entonces para descifrar la clave simétrica 14A del título de libro electrónico, la cual, a su vez, se usa para descifrar la secuencia de contenido 16 del título de libro electrónico. El procesamiento continúa en la etapa 188.

Si, en la etapa 176, se determina que esta activación es una recuperación, entonces (en la etapa 178) se generan unos certificados de activación con la información que se almacenó en la etapa 186, y el procesamiento continúa en la etapa 188.

En la etapa 188, los servidores de activación generan y firman digitalmente un ejecutable de repositorio seguro individualizado (que está unido al ID de máquina subido) y un certificado de activación (que está unido al ID de PASSPORT™ del usuario). Entonces, el ejecutable de repositorio seguro y el certificado de activación se descargan al cliente (las etapas 188 y 190). El certificado de activación se cifra (por razones de privacidad) y es subido más adelante por el cliente al servidor de descarga para preparar copias completamente individualizadas (títulos con protección de nivel 5). El ID de PASSPORT™ del usuario se puede cifrar y marcar en el Registro del PC como parte de esta descarga, para la subida durante transacciones comerciales. Este procedimiento puede asegurar que el ID de PASSPORT™ que está incluido en el URL para la descarga coincide con el del certificado de activación que está incluido en el cuerpo del Post, para evitar el robo de contenido.

En la etapa 192 se determina si la descarga tuvo éxito. En caso negativo, se registra un evento y la descarga se intenta de nuevo (las etapas 194 y 192). Si la descarga tuvo éxito, entonces en la etapa 196, se proporciona una "página de enhorabuena" al usuario y se le notifica que la activación ha sido completada. La "página de enhorabuena" también puede proporcionar un vínculo para canjear libros promocionales gratuitos en este momento, como una forma de alentar a los usuarios a activar sus lectores. Este vínculo puede sacar partido de un procedimiento que es expuesto por el Control de ActiveX de Activación para devolver al usuario a una página de biblioteca en el lector. Entonces, el procedimiento finaliza en la etapa 198.

Es preferible que, una vez que el lector ha conectado con los servidores de activación 94, los servidores 94 conduzcan la totalidad de la experiencia del usuario por medio de páginas de ASP y de HTML. Estas páginas preferiblemente son conformes a una especificación convencional, y usarán la guía de estilo y procedimientos de secuencias de comandos de java que se proporcionan para asegurar una experiencia sin interrupciones, esto es consistente con el "aspecto y la sensación" de la interfaz de usuario del lector.

Parte del procedimiento de activación para el lector de plataforma abierta (por ejemplo, una aplicación de soporte lógico de lector instalada en un PC) es la individualización de repositorio seguro y la descarga posterior. Tal como se analiza con mayor detalle en el documento con n.º de expediente del mandatario MSFT-0126, presentado de forma simultánea con el presente documento, se proporciona un componente de servidor (por ejemplo, el servidor de repositorio seguro 100, que se muestra en la figura 4) que es responsable de individualizar módulos de soporte lógico de repositorio seguro en cada instancia del lector para plataformas abiertas (por ejemplo, ordenadores portátiles y de escritorio). El repositorio seguro único oculta las claves criptográficas que se usan en el procedimiento de eliminación de sello y descifrado de archivos de LIT de nivel 5, así como de asegurar que los documentos con contenido de nivel 5 descifrados no escapen del sistema controlado y, debido a que el mismo está individualizado para una instalación de soporte físico particular, este resiste la portabilidad y, en el caso de que se rompiera, su individualización resiste el uso de las mismas técnicas de rotura sobre un repositorio seguro diferente instalado en un soporte físico diferente.

Tal como se ha hecho notar en lo que antecede, un aspecto de resistir el abuso del sistema de DRM es limitar el número de activaciones que cualquier usuario particular puede tener con un ID de PASSPORT™ único. Si este número no está limitado, los usuarios deshonestos pueden ser capaces de suscribirse a un PASSPORT™ de "dominio público" a continuación compartir las credenciales para esa cuenta con la totalidad de sus amigos (o lo que es peor, publicar esta en la web), junto con todos los libros electrónicos que compraron estos. Esto creará rápidamente una cadena de piratería, debido a que cualquier usuario que active el lector con las credenciales de PASSPORT de "dominio público" podría leer entonces títulos de nivel 5 individualizados para esa cuenta de "dominio público".

Por lo tanto, de acuerdo con una característica de la invención, es deseable tener unas "cuotas" de activación que permitan que los usuarios activen lectores en múltiples dispositivos que son propiedad de estos (por ejemplo, un ordenador portátil, un ordenador de escritorio, PocketPC, libro electrónico, etc.) así como que permitan que los mismos activen nuevos dispositivos a medida que los mismos actualizan su soporte físico, vuelven a dar formato a sus discos duros, etc., sin permitir unas activaciones no controladas e ilimitadas de lectores para las mismas credenciales de PASSPORT. La experiencia pasada con el comportamiento de los usuarios sugiere que los usuarios legítimos activan un lector (o un pequeño número de lectores) inicialmente y, entonces, pueden activar nuevos lectores de forma ocasional pero no es probable que activen nuevos lectores con tanta frecuencia como cada día o cada semana. Para posibilitar estos usos legítimos del sistema de activación, al tiempo que se previene el abuso, el número de activaciones para un usuario dado (un ID de PASSPORT™) se aumentará de forma periódica, hasta un máximo definido (el cual será, por ejemplo, de cinco activaciones inicialmente). A medida que el usuario activa nuevos dispositivos, baja su cuota de activaciones disponibles. A medida que pasa el tiempo, el número se aumenta, a una tasa sugerida de, por ejemplo, una activación adicional cada 90 días (a partir de la fecha de la primera activación) hasta que el número alcanza 10. Este tipo de límite permitirá que los usuarios activen lectores (o reactiven, póngase por caso, lectores antiguos en dispositivos con discos duros a los que se ha vuelto a dar formato) con una frecuencia razonable, y resistirá el abuso del sistema por "piratas".

Los servidores de activación 94 imponen el límite a las activaciones mediante el almacenamiento, en la base de datos de activación 102, de una lista de todas las activaciones que ha solicitado un ID de PASSPORT™ dado, junto con sus marcas de fecha. Si se realiza una solicitud de reactivación, la cuota no se ve afectada, siempre que el ID de máquina (por ejemplo, el número único que une el repositorio seguro al soporte físico que aloja el lector) sea la misma (debido a que esto no daría como resultado un robo, debido a que se está activando de nuevo el mismo PC).

Flujo de procedimiento de comercio electrónico

Una visión de conjunto del procedimiento básico mediante el cual unos títulos de libros electrónicos se adquieren y se entregan en línea se describe a continuación con referencia a la figura 9. Usando un navegador o las "páginas de librería" o el lector 90 o 92, el usuario elige un libro o libros por medio de unos mecanismos que implementa el sitio de comercio al por menor (la etapa 200). El usuario entonces paga por los títulos, si se requiere un pago (la etapa 202). La transacción concluye en la etapa 204 con una página de recibo (es decir, una página de confirmación de pedido o de "gracias") que contiene vínculos (solicitudes de POST) para descargar cada título comprado (es decir, los URL que contienen la dirección del servidor de contenido 76, más la información cifrada que es creada por el objeto de cifrado de URL 74). Para las copias completamente individualizadas (el nivel 5), una secuencia de comandos de lado de cliente rellenará el cuerpo del POST con el certificado de activación, preferiblemente usando un objeto de COM que es implementado por el lector que obtiene el certificado de activación necesario o una información relevante a partir del mismo.

Tras pulsar sobre cualquiera de los vínculos en la etapa 206, el navegador inicia una descarga a partir de los servidores de contenido 76 (por medio de la DLL de ISAPI de servidor de descarga 78). Para las copias selladas de

forma individual (de exlibris (por ejemplo, de nivel 3)), el servidor de descarga 76 añade el nombre del consumidor a los metadatos del título y vuelve a sellar la clave simétrica 14A usando una nueva función criptográfica de troceo que resulta de los nuevos metadatos, los cuales incluyen ahora el nombre del usuario. Para las copias completamente individualizadas (el nivel 5) una licencia se genera y se incrusta en el archivo de LIT, además del exlibris que se está creando. Esta licencia contiene la clave simétrica 14A que cifró el archivo de LIT "sellado" con la clave pública en el certificado de activación. Cuando la descarga ha sido completada (la etapa 208), el servidor de descarga 76 registra la transacción y, en el cliente, el lector se lanza de forma automática (la etapa 210). El título se puede mover a una carpeta "Mi Biblioteca" (por ejemplo, en un PC que usa uno de los sistemas operativos WINDOWS de MICROSOFT, una carpeta de este tipo se podría denominar C:\MiBiblioteca, y se reservaría para el almacenamiento de archivos de LIT). El libro electrónico se abre por su página de portada y el nombre del propietario legítimo se presenta bajo el nombre del autor.

El procedimiento de comercio electrónico se detalla adicionalmente en la figura 10 con referencia específica a los componentes del sistema de DAS. En la etapa 1, el cliente 90 o 92 realiza una solicitud de POST a la DLL de ISAPI de servidor de descarga 78. El cuerpo de esta solicitud de publicación contendrá, como mínimo, el blob cifrado que es generado por el objeto de cifrado de URL 74. Para las copias completamente individualizadas (con protección de nivel 5), esta solicitud de publicación también contendrá el certificado de activación que se requiere cuando se sella la licencia de XrML (véase más adelante).

Durante la etapa 2, la ISAPI 78 extrae, del cuerpo del POST, el ID de comerciante minorista, el cual se requiere para capturar la clave simétrica 75 que está asociada con este comerciante minorista para descifrar el URL. Entonces, este descifra y valida la solicitud de descarga. Si la solicitud es no válida y / o el TTL que se ha computado ha expirado (por ejemplo, un posible ataque de reproducción), el servidor de descarga puede redirigir el navegador de vuelta al sitio de librería. El sitio de librería 71 siempre debería estar encapsulado en la variable de servidor HTTP REFERRER. Durante esta etapa, un nombre de archivo sencillo opcional se puede proporcionar por medio del blob cifrado. Esta cadena, cuando se devuelve, será usada por la ISAPI como el nombre de archivo cuando se descarga el título de LIT al usuario final.

En la etapa 3, la ISAPI 78 pasa el ID de libro y el tipo de ID de libro al módulo de complemento de almacén de contenido, el cual devuelve entonces la ubicación física del archivo de LIT en el almacén de contenido en base a o bien una entrada de memoria caché (si el archivo de LIT que se está solicitando se hubiera descargado previamente) o bien una consulta en la base de datos de cumplimiento 89.

En la etapa 4, si el ID de libro no es hallado en la memoria caché local de la ISAPI 78, el archivo de LIT se recupera del almacén de contenido 80 y se copia en la memoria caché local de la ISAPI. Cuando la ISAPI almacena en memoria caché los archivos de LIT de forma local, esta despoja los archivos de LIT de sus claves simétricas 14A y las almacena en un depósito de memoria caché separado, las indexa mediante su ID respectivo, lo que puede aumentar la seguridad.

En la etapa 5 la ISAPI 78 realizará una de estas posibles etapas de acuerdo con el nivel de DRM que se requiere para el archivo de LIT que se está descargando:

> Si la solicitud es para un archivo de nivel 1 de DRM, o el archivo de LIT no se ha sellado en fuente en el almacén de contenido 80, la ISAPI preferiblemente devuelve un error, indicando eso la condición de error apropiada (una solicitud no válida o un título no válido en el almacén de contenido, de forma respectiva).

Para los títulos sellados por la fuente (el nivel 2), la ISAPI devuelve el archivo al usuario final, sin procesamiento realizado sobre el archivo en modo alguno. Esto es similar a la descarga de cualquiera de los otros archivos estáticos.

Para los títulos sellados de forma individual (el nivel 3), el nombre del usuario se insertará en una nueva secuencia en el archivo de LIT, los metadatos marcados con el nivel 3 (para su uso por el cliente de lector 90 o 92), se aplica una función de troceo a los nuevos metadatos, y la clave simétrica 14A que se usa para cifrar el archivo de LIT se sella con el nuevo valor de función criptográfica de troceo que se ha computado.

Para los títulos completamente individualizados (el nivel 5), la ISAPI 78 realizará, además de la generación de las funciones que se han hecho notar en lo que antecede para el nivel 3, la publicación de una solicitud en el módulo de concesión de licencia 77, el cual generará un blob de XrML de licencia, firmará este con el certificado del centro de cumplimiento, lo sellará con la clave pública de activación del usuario final y lo devolverá para su incrustación en el archivo de LIT.

Para ambos niveles 3 y 5, todo el procesamiento se lleva a cabo en el espacio de memoria temporal que se crea durante la etapa 4. Este espacio de memoria será descartado posteriormente por la ISAPI, cuando la descarga haya sido completada.

En la etapa 6 la DLL de ISAPI devuelve el archivo de LIT al servidor IIS 76 para la descarga. Si, durante la etapa 3, el módulo de complemento de almacén de contenido devolvió una cadena de "nombre sencillo", este valor se usa en el encabezado de HTTP como el nombre de archivo que se va a almacenar en la máquina del usuario.

En la etapa 7 el archivo de LIT se descarga mediante IIS al usuario final por medio de HTTP. Cuando la descarga ha sido completada, IIS devolverá la llamada a la DLL de ISAPI 78 para notificar que se dio cumplimiento a la solicitud pendiente y se cerró la conexión. La ISAPI 78 purgará entonces toda la memoria temporal que se usa durante la etapa 5.

En la etapa 8, la DLL de ISAPI 78 usará la canalización de cumplimiento asíncrona (por medio del cliente independiente de MSMQ local 86) para registrar la transacción en la base de datos de registro 91 para la notificación y / o facturación posterior. Esta canalización también se usa para invalidar entradas de memoria caché en la memoria de la ISAPI de forma asíncrona, de tal modo que cualesquiera modificaciones al almacén de contenido 80 que sean realizadas por la herramienta de gestión de contenidos 82 darán lugar a que la ISAPI invalide los datos almacenados en memoria caché y recurra al módulo de complemento 88 (y posteriormente el almacén de contenido 80) para recuperar el archivo de LIT para la entrada de memoria caché invalidada.

Una vez que el título de libro electrónico se ha descargado en el cliente (después de la etapa 7), se puede lanzar el cliente de lector. Esto se posibilita por medio de una asociación de extensión de archivo de LIT con el lector. El lector puede mover el archivo a la carpeta de biblioteca local (por ejemplo, "C:\MiBiblioteca") y abrir el libro por su página de portada, la cual para los títulos de nivel 3, identifica claramente al propietario por debajo del nombre del autor.

Funcionalidad de gestión de contenidos

Una de las etapas al asegurar el contenido en un entorno de DRM es el pre-cifrado de los archivos de fuente (archivos de LIT) usando las claves simétricas 14A que son generadas por la herramienta de cifrado. Este procedimiento posibilita que el servidor de descarga 76 selle la clave simétrica 14A de acuerdo con los requisitos de cada nivel de DRM. El centro de cumplimiento 73 es responsable de rellenar el almacén de contenido 80 de acuerdo con su infraestructura de codificación y de catalogación existente. El centro de cumplimiento 73 también es responsable de comunicar el ID de libro, el tipo de ID de libro y sus metadatos asociados a los comerciantes minoristas que alojan unas librerías que señalan el sitio del proveedor de contenido para el cumplimiento.

De acuerdo con una característica de la presente invención, puede existir independencia entre el servidor de descarga 76 y los servidores de almacén de contenido 80 del centro de cumplimiento. Cada par de ID de libro / tipo de ID de libro que viene en el URL que es provisto por los comerciantes minoristas 71 se resolverá para dar una ruta física hasta un archivo de LIT por medio del módulo de complemento de almacén de contenido 88, el cual puede ser personalizado por cada centro de cumplimiento 73. Esto prevé una máxima flexibilidad y escalabilidad del repositorio de almacén de contenido así como la DLL de ISAPI de servidor de descarga 78.

Una base de datos de librería (comerciante minorista) se rellena con los ID de libro que son generados por una herramienta para gestionar los archivos de LIT del centro de datos de un proveedor de contenido particular. Se supone que este procedimiento tiene lugar de forma asíncrona y por medio de un acuerdo contractual entre el comerciante minorista 71 y el proveedor de contenido (el centro de cumplimiento) que aloja los servidores de contenido 76. Estos ID se proporcionarán a la DLL de ISAPI de servidor de descarga 78 por medio del URL (en la porción cifrada del URL).

Consideraciones de diseño

Se describen en lo sucesivo unos esquemas a modo de ejemplo para las diversas tablas que se usan en las bases de datos de DAS. Los esquemas a modo de ejemplo no han de considerarse como limitantes de la presente invención, debido a que son posibles otros esquemas.

Base de datos de cumplimiento

Hay tres tablas en la base de datos de cumplimiento a modo de ejemplo. Estas incluyen una tabla DAS_Product que contiene la totalidad de la información que se requiere para procesar una solicitud de descarga, una DAS_Registered_Retailers que contiene la totalidad de la información acerca de los comerciantes minoristas a los que se permite dar cumplimiento a títulos usando esta instalación de cumplimiento de DAS, y una DAS_Licensor_Config que contiene la Licencia requerida del Emisor de Licencia que es provista por Microsoft para cada Socio de instalación de DAS. NO hay relación alguna que se requiera entre estas tablas; no obstante, si son necesarias unas relaciones entre tablas, entonces se usan los identificadores únicos (claves primarias) de cada tabla.

Tabla DAS_Product

```
(
        DAS_BookID_Path_Mapping_ID int not null IDENTITY(1,1),
        BookID varchar(256) not null, -- ejemplo "0-201-63446-5"
        BookIDType varchar(32) not null, -- ejemplo "ISBN"
        Title varchar(256) not null, -- ejemplo "Tarzán de los monos"
        Publisher varchar(256) not null, -- ejemplo "Libros Ballantine"
        UNCPath varchar(256) not null, -- ejemplo "\\Store\tarzan.lit"
        Price varchar(32) not null, -- ejemplo "6,59"
```

```
        PriceStructure varchar(32) not null, -- ejemplo "Retail"
        Currency varchar(10) not null, -- ejemplo "USD"
        SecurityLevel varchar(32) not null, -- ejemplo "5"
        DateUpdated datetimenull DEFAULT (getDate()), -- última vez que se actualizó la fila
        DateCreated datetimenull DEFAULT (getDate()) -- momento en el que se creó la fila
        )
```

Tabla DAS_Registered_Retailers

Esta tabla contiene el ID de comerciante minorista y la cadena secreta que se usa cuando se computa la clave simétrica 75 que se usa para cifrar / descifrar los URL para el cumplimiento. Cada cadena ha de coincidir con la cadena que es usada por el comerciante minorista cuando se instala el objeto de COM de cifrado de URL, debido a que así es como se autentica cada solicitud de descarga.

```
(
        DAS_Registered_Retailers_ID int not null IDENTITY(1,1),
        RetailerID varchar(256) not null, -- ejemplo "Comerciante minorista-111-888"
        RetailerName varchar(256) not null, -- ejemplo "Bames and Noble"
        RetailerDesc varchar(4096) not null, -- ejemplo "Comerciante minorista de libros"
        SharedSecret varchar(256) not null, -- ejemplo "Haciendo_Posibles_Libros_Electrónicos"
        DateUpdated datetime null DEFAULT (getDate()),
        DateCreated datetime null DEFAULT (getDate())
        )
```

Tabla DAS_Licensor_Config

Esta tabla contiene los ajustes de configuración para el componente de concesión de licencia del servidor de descarga. Cuando el servidor comienza, el certificado del emisor de licencia y la clave privada del emisor de licencia se leen de esta tabla y se usan para generar licencias de nivel 5 para archivos de LIT. Es preferible almacenar esta información acerca del servidor de SQL debido a que los datos son demasiado grandes para almacenarse en el registro local del servidor de descarga, y debido a preocupaciones de seguridad de que la clave privada de los comerciantes minoristas se pueda ver comprometida si se almacena en un archivo plano. Esta también prevé cambios fáciles en los parámetros de configuración de los servidores de descarga, debido a que los socios de DAS solo han de modificar esta tabla en la base de datos de cumplimiento 89 y todos los servidores de descarga recogerán el cambio (por medio del componente de canalización de cumplimiento y de mensajería asíncrona), simplificando la gestión.

```
(
        DAS_Licensor_Config_ID int not null IDENTIFY(1,1),
        LicensorCertificate varchar(4096) not null, -- certificado del emisor de licencia
        firmado
        LicensorPrivateKey varbinary(350) not null, -- forma binaria de la clave privada del
        emisor de licencia
        DateUpdated datetime null DEFAULT (getDate()),
        DateCreated datetime null DEFAULT (getDate())
        )
```

Base de datos de registro

La base de datos de registro 91 se usa para el registro de todas las solicitudes de descarga. A medida que los servidores de descarga procesan solicitudes, la canalización de cumplimiento asíncrona (en base al servidor de Cola de Mensajes de MICROSOFT®) se usa para escribir, por medio de un objeto de COM que reside en el servidor de base de datos de cumplimiento, cada mensaje procedente de la cola en la tabla DAS_Log. Esto permitirá que los sitios de DAS auditen su cumplimiento y determinen cuántas descargas tuvieron lugar, y cuando, y cuáles son los títulos descargados con más frecuencia, etc. Esta tabla también se puede usar para fines de facturación. La base de datos de registro comprende una única tabla (DAS_Log) que contiene la totalidad de las anotaciones de registro de transacción a partir de títulos descargados.

```
(
        DAS_Log_ID int not null IDENTITY(1,1),
        BookId varchar(64) not null, -- ejemplo "0-201-63446-5"
        BookIdType varchar(32) not null, -- ejemplo "ISBN"
        SecurityLevel varchar(32) not null, -- ejemplo "5"
        NameOfFile varchar(256) not null, -- ejemplo "Alice30.lit"
        CustomerID varchar(256) not null, -- ejemplo "34235433"
        UserName varchar(256) not null, -- ejemplo "Pavel Zeman"
        TransactionId varchar(256) not null, -- ejemplo "123-456-789"
        License varchar(4096) null, -- solo para contenido de nivel 5 - texto de la Licencia
        RetailPrice varchar(32) null, -- ejemplo "6,59 $"
        Cost varchar(32) null, -- ejemplo "5,59 $"
        MSRP varchar(32) null, -- ejemplo "7,59 $"
        DownloadAgentvarchar(256) null, -- ejemplo "Mozzilla"
```

```
IPAdress varchar(32) null, -- ejemplo "123.456.789.000"
DateLogged datetime null DEFAULT (getDate())
)
```

Base de datos de activación

La base de datos de activación 102 aloja la totalidad de la información requerida para activar lectores así como una información de configuración para operar los servidores de activación. Hay cinco tablas en la base de datos de activación. La tabla Key_Pairs contiene los pares de claves que se usan cuando se generan unos certificados de activación. La tabla Users aloja las credenciales de PASSPORT™ para cada usuario activado, junto con el ID de par de claves (un vínculo a la tabla Key_Pairs) y la fecha de la primera activación. UsersDevices es una lista de todos los ID de soporte físico (es decir, los ID de máquina) que son activados por todos los usuarios. Con el fin de identificar a qué máquina se está haciendo referencia, esta tabla tiene una restricción de clave primaria sobre UserNum (una representación interna de cada usuario en la tabla Users) y MachID (el ID de máquina computado). La KeyPtr realiza un seguimiento del número de pares de claves que se usan a partir de la tabla Key_Pairs. Esta también señala el siguiente par de claves disponible a usar. La AS_DB_Config contiene elementos de configuración para la base de datos y los servidores de activación 94.

Tabla Key_Pairs

```
(
   ID_Key_Pair int not null UNIQUE IDENTITY(1,1),
   PublicKey KeyValue not null,
   PublicKeyXML KeyValue not null,
   PrivateKey KeyValue not null,
   BinaryPrivateKey BinKeyValue not null,
   AssignedToReader tinyint null DEFAULT(0),
            /* vínculo a UsersDevices.ID_UsersDevice */
   DateAssigned smalldatetime null DEFAULT (NULL),
   DateCreated smalldatetime null DEFAULT (getDate())
   )
```

Tabla Users

```
(
   UserNum int not null UNIQUE IDENTITY(1,1),
   FullName varchar(60) null,
   Email varchar(60) null,
   UserId varchar(60) not null PRIMARY KEY,
   DateMade smalldatetime null DEFAULT (getDate()),
   ID_KeyPair int not null
   )
```

Tabla de UserDevices

```
(
   UsersDeviceNum int not null UNIQUE IDENTITY(1,1),
   MachId varchar(255) not null,
   UserNum int not null,
   DateRegistered smalldatetime null DEFAULT (getDate()),
   ID_KeyPair int not null,
   TimesRegistered int null DEFAULT (0),
   CONSTRAINT PC_UNQ PRIMARY KEY (UserNum, MachId)
   )
```

Tabla KeyPtr

```
(
   NextKeyToUse int not null
   )
```

Tabla AS_DB_Config

```
(
            /* cuando el número de claves libres cae por debajo de este número, un trabajo
            programado de GenKey está añadiendo claves */
            MinKeysAvailable int not null,
            /* inicialmente el usuario puede activar todos estos PC */
            MaxPCperUser int not null,
            /* si el usuario alcanzó el límite en lo que antecede, pero este periodo ha
            transcurrido desde su última activación, el usuario puede añadir uno más */
            GrantExtraPCPeriodlnDays int not null,
            /* para evitar ataques de DOS (denial of service, denegación de servicio) mediante la
            reactivación del mismo PC una y otra vez, este se puede establecer en producción a un
```

```
            valor bajo (por ejemplo 3), pero una prueba lo puede establecer a alto para las
            pruebas de esfuerzo */
            MaxSamePCregistrations int not null
    )
```

Almacenamiento de DRM dentro de archivos de LIT

Cada archivo de LIT es, en efecto, un pequeño sistema de archivos, que consiste en una colección de elementos de almacenamiento y sus secuencias asociadas. En la raíz de cada archivo de LIT es un objeto de almacenamiento dedicado para DRM. Las subsecuencias del objeto de almacenamiento de DRM variarán dependiendo del nivel de DMR por medio del cual se distribuyó el archivo de LIT. En un archivo de LIT con protección de nivel 5, un Almacén de Datos contiene el contenido real del libro electrónico, y un Almacén de Almacenamiento de DRM contiene todos los datos binarios específicos de DRM. La Tienda de Almacenamiento de DRM incluirá unas secuencias de ValidationStream, de DRMSource y de DRMSealed (para copias selladas por la fuente y selladas de forma individual). Para los títulos completamente individualizados, el archivo de LIT también incluirá la secuencia de licencias, la cual incluye una licencia de usuario final (EUL, *End-User-License*).

Formato de Licencia

En lo sucesivo se da una Licencia a modo de ejemplo, la cual se usa para cada descarga de títulos completamente individualizados. La licencia es una construcción que define los derechos que puede ejercer el usuario tras la compra del título, además de definir los requisitos para eliminar el sello de la clave simétrica para ejercer esos derechos. Son ejemplos de "derechos" que se podrían representar en la licencia la presentación del contenido (por ejemplo, en el ejemplo de contenido de texto, la lectura del mismo en el monitor de un PC), la impresión del contenido, o el copia - y - pega porciones del contenido. Se hace notar que el formato de licencia a modo de ejemplo no tiene por objeto limitar el ámbito de la presente invención debido a que son posibles otros formatos de licencia que tienen más o menos información, al igual que lo son las licencias que tengan una información de licencia en diferentes formatos.

Es preferible que el lenguaje elegido para representar una Licencia sea XML, y el formato de la Licencia esté basado en la especificación de Lenguaje de Marcado de Derechos Extendido (XrML, *Extended Rights Markup Language*). Este es un lenguaje de marcado muy adecuado para describir los derechos de uso de una forma flexible. XrML también prevé una gran interoperabilidad y puede prever que se saque partido a largo plazo de cualesquiera inversiones tecnológicas realizadas sobre los componentes que generan y gestionan estas licencias. En una realización preferida, solo se conceden a la licencia aquellos que se expresan en la licencia - es decir, si un derecho no se concede de forma expresa, este se deniega. No obstante, será apreciado por los expertos en la materia que son posibles otras disposiciones, tal como en donde se presume un conjunto por defecto de derechos a menos que sea denegado o modificado de forma expresa por la licencia.

Las etiquetas del nivel más alto en un formato contraído son tal 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 implícito
             ======================================
                   Derechos de uso del libro
          - <!-- ====================================
            -->
          - <! -- Emisor de Licencia del libro
            -->
          - <!-- ================================
            -->
          + <LICENSOR>
          - <!-- ================================
            -->
          - <! -- Titulares de licencia del libro
            -->
          - <!-- ======================================
            -->
```

```
+ <LICENSEDPRINCIPALS>
  </BODY>
- <!-- ====================================
  -->
- <!-- Firma del cuerpo de la Licencia
  -->
- <!-- ========================================
  -->
+ <SIGNATURE>
</XrML>
```

La primera línea de la estructura de XrML en lo que antecede define la versión del lenguaje XML que se usa para crear la licencia de XrML. La segunda línea especifica el nombre del archivo de DTD que se usa para analizar sintácticamente el archivo de XML. La etiqueta de BODY proporciona el tipo de licencia, la versión de la especificación de XrML usada cuando se generó la licencia, y la fecha en la que se emitió la misma. Esta también es la metaetiqueta para la totalidad de la licencia, la cual tiene las siguientes subsecciones: WORK, LICENSOR, LICENSEDPRINCIPALS, y SIGNATURE. WORK contiene la totalidad de la información semántica acerca de la licencia, incluyendo los DERECHOS de uso. Los contenidos de este campo (incluyendo las etiquetas) constituyen los datos a los que se aplica una función de troceo y que se firman. LICENSOR contiene una información en relación con la entidad que emitió la licencia, por lo general un comerciante minorista. LICENSEDPRINCIPALS contiene una serie de entidades de seguridad que se han de autenticar cuando se ejercen los derechos de uso que se especifican en una licencia. SIGNATURE contiene la función de troceo / resumen de la LICENSEBODY así como una información acerca de cómo se creó la función de troceo, incluyendo el algoritmo usado. Esta también incluye el DIGEST codificado de acuerdo con el algoritmo nombrado por el Emisor de Licencia cuando se emite la Licencia. Las etiquetas de DIGEST y de SIGNATURE proporcionan la información de autenticación que se usa para validar la totalidad de la licencia de una forma que no se puede manipular indebidamente.

Estructura de la etiqueta de BODY

La etiqueta principal de una construcción de licencia de XrML es la etiqueta de BODY, la cual 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>Un libro de Jaime</NAME>
      </OBJECT>
      <CREATOR type="author">Jaime primero</CREATOR>
      <CREATOR type="author">Jaime segundo</CREATOR>
    - <OWNER>
      - <OBJECT type="Person">
          <ID type="US-SSN">103-74-8843</ID>
          <NAME>Mike el hombre</NAME>
          <ADDRESS type="email">mike@man.com</ADDRESS>
        </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+aDjgYL
                xwrktqFDR4HZeIeR1g+G5vmKNZRt
                9FH4ouePWz/AJYnn2NdxoJ6mcIIAQ
                Ve6Droj2fxA== </VALUE>
          </PARAMETER>
        </PUBLICKEY>
```

```
  </OWNER>
- <!-- ========================================== -->
- <!-- Componentes del libro
     -->
- <! -- Un capítulo, y una imagen con valor implícito -->
- =!-- ========================================== -->
- <PARTS>
   - <WORK>
      - <OBJECT type="Chapter">
           <ID type="relative">0</ID>
           <NAME>Capítulo 1</NAME>
        </OBJECT>
     </WORK>
   - <WORK>
      - <OBJECT type="Image">
           <ID type="relative">1</ID>
           <NAME>Imagen 1: Photon Celebshots
               Dogs</NAME>
        </OBJECT>
      - <DIGEST sourcedata="LicensorMeta">
           <ALGORITHM>SHA1</ALGORITHM>
         - <PARAMETER name="codingtype">
              <VALUE
                  encoding="string">surfacecoding</VALUE>
           </PARAMETER>
           <VALUE encoding="base64"
               size="160">OtSrhD5GrzxMeFEm8q
               4pQlCKWHI=</VALUE>
        </DIGEST>
     </WORK>
  </PARTS>
- <!-- ========================================== -->
- <!-- Derechos de uso del libro
  -->
- <!-- ========================================== -->
- <RIGHTSGROUP name="Derechos principales">
     <DESCRIPTION>Un cierto 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== </VALUE>
              </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 isocode="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>
        - <!--==================================== -->
        - <!-- Emisor de Licencia 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>
- <!-- ====================== -->
- <!-- Titulares de licencia del libro -->
- <!-- ====================== -->
- <LICENSEDPRINCIPALS>
  - <PRINCIPAL>
    - <OBJECT type="program">
        <ID type="msprogid">XrML.interpreter</ID
        >
        <NAME>INTÉRPRETE DRPL</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="signaturekey">
        - <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>Ordenador de John</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">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>
                  - <VERIFICATIONDATA>
                     - <PARAMETER name="bbid">
                          <VALUE
                           encoding="string">xxzzy</VAL
                           UE>
                      </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>Lector de Libros de MS 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">bXIwYXNzd29yZA=
                         =</VALUE>
                </DIGEST>
              </VERIFICATIONDATA>
            </AUTHENTICATOR>
          </PRINCIPAL>
        </LICENSEDPRINCIPALS>
        </BODY>
```

Autenticidad de Licencia

Tal como se ha mencionado en lo que antecede, el repositorio seguro de lector autentica una licencia por medio de las etiquetas de SIGNATURE y de DIGEST. Esto es de tal modo que el soporte lógico de cliente puede validar que el contenido que se está presentando provino de una fuente de confianza. Un ejemplo más detallado de estas etiquetas se proporciona en lo sucesivo:

```
- <!--================================
          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">OtSrhD5GrzxMeFEm8q4pQlCKW
                HI=</VALUE>
            </DIGEST>
            <VALUE encoding="base64"
                size="512">A7qsNTFT2roeL6eP+IDQFwjIz5XSFBV
                +NBFOeNa7de+1D6n+MPJa3J7ki8Dmwmuu/pBciQ
                nJ4xGaqRZ5AYoWRQ== </VALUE>
        </SIGNATURE>
```

Escenarios de fuentes de contenido de sistema de DRM

El contenido de fuente se distribuye preferiblemente en un formato de libro electrónico abierto ("OEB", *Open eBook*), el cual será personalizado más adelante por el comerciante minorista en cada Lector objetivo. El formato de OEB se especifica en el documento con título *Open eBook™ Publication Structure* 1.0, con fecha 16 de septiembre de 1999, el cual se encuentra disponible en http://www.openebook.org.specification.htm.

Escenarios de fuentes de contenido

Dentro del contexto del sistema de DRM, se espera que las fuentes de contenido (autores y / o editores) de libros electrónicos proporcionen unas copias o bien abiertas (es decir, sin escala) o bien a escala que estén listas para la venta. Con el fin de ser distribuidos por el servidor que se describe en lo sucesivo, los editores han de proporcionar copias que, como mínimo, se hayan sellado en fuente, o como alternativa, opcionalmente los editores pueden proporcionar unos archivos de OEB / HTML de fuente que el comerciante / distribuidor cifrará y almacenará para el cumplimiento. Las fuentes de contenido también pueden proporcionar un archivo separado (por ejemplo, XML, texto, secuencia de comandos de base de datos, etc.) que proporcionará una información específica del comerciante acerca de cada título que se está distribuyendo, la cual será usada por el comerciante / distribuidor para rellenar sus bases de datos de cumplimiento. Tal información puede incluir el nivel de DRM deseado, precios, señuelo, etc.

Debido a que existe una expectativa de que una relación de confianza entre los editores y los comerciantes minoristas se mantenga preferiblemente de forma contractual y no de manera tecnológica, en general no es necesario el cifrado y / o sellado de títulos entre los editores y los comerciantes / distribuidores. Una relación de este tipo prevé una implementación más simple. Si, no obstante, la seguridad añadida es una preocupación, la presente invención prevé títulos que se pueden cifrar cuando se transfieren entre los editores y los comerciantes / distribuidores.

De acuerdo con la presente invención, los editores pueden distribuir el contenido a los comerciantes minoristas por medio de uno de entrega de un medio de almacenamiento masivo portátil (CD, DVD, etc.); servidores de FTP seguros o bien en el editor o bien en el sitio de comerciante / distribuidor; HTTPS seguro (SSL) o bien en el editor o bien en el sitio de comerciante / distribuidor; y conexiones de red dedicadas seguras entre el editor y los sitios de comerciante / distribuidor.

Escenarios de comerciante / distribuidor

A continuación se describirán varios escenarios de distribución no limitantes. Los escenarios tienen por objeto proporcionar ejemplos de las ventas a los clientes, y no tiene por objeto limitar la presente invención debido a que son posibles otros escenarios.

Ventas de las copias selladas por la fuente

Después de que el cliente que realiza la compra haya seleccionado los títulos que desea comprar y decida completar un pedido, el comerciante procesará el pedido de acuerdo con sus procedimientos existentes (por ejemplo, validación de tarjeta de crédito, facturación, etc.). Esto puede incluir requerir que los usuarios se autentiquen a sí mismos (para aquellos que requieran una anotación de pertenencia de sus clientes) o simplemente cumplimenten un formulario de pedido. A continuación, el comerciante generará y descargará un recibo (prueba de compra electrónica) al cliente que realiza la compra. Tal como se ha hecho notar en lo que antecede, es preferible que el recibo electrónico incluya la totalidad de la información que se requiere para posibilitar que el usuario descargue más adelante los títulos que este compró por medio de un mecanismo tal como un URL que señala el servidor de contenido 76 y contiene el blob cifrado que es generado por el objeto de cifrado de URL. Una vez que el usuario ha pulsado sobre el URL que está incluido en el recibo electrónico para descargar el título comprado, el servidor que se enumera en ese URL (es decir, el servidor de cumplimiento o de contenido) descarga el título al que se ha hecho referencia en el comprador. Los servidores de contenido / descarga 76 pueden validar que, de hecho, el pedido fue realizado por el usuario que intenta descargar el título.

Tal como se ha mencionado previamente, las copias selladas por la fuente pueden incluir de forma indeleble el nombre del editor y / o autor y cualesquiera otros derechos que se hayan delegado al comerciante como parte del procedimiento de distribución. El comerciante / distribuidor usa unas herramientas para cifrar el título con una clave simétrica 14A que es provista por esas herramientas. Estas mismas herramientas cifrarán la clave simétrica 14A con

una función criptográfica de troceo de los metadatos del título e incrustarán la clave simétrica cifrada 14A en una secuencia separada en el título. Cuando el soporte lógico de lector abre estos títulos, este aplicará el mismo algoritmo que es usado por la herramienta para descifrar la clave simétrica y, entonces, lo usará para descifrar el contenido. Se hace notar que los títulos comprados de esta forma pueden ser redistribuidos fácilmente por los usuarios finales (por ejemplo, mediante la publicación del archivo de LIT en la web, o mediante el guardado de este en el disco magnético 29 o el disco óptico 31 y el envío del disco a otro usuario); por lo tanto, se recomienda que el comerciante proporcione advertencias que conciernen a la distribución ilegal en cada recibo. Se alienta a los propietarios de títulos vendidos de esta forma a incluir una información de derechos de autor como parte de la publicación.

Ventas de copias selladas de forma individual

Similares a las copias selladas por la fuente, las copias selladas de forma individual (por ejemplo, el nivel 3) requieren que el comerciante minorista nombre el propietario legítimo del título en los metadatos y, entonces, selle la clave simétrica 14A que se usa para el cifrado / descifrado del contenido con una nueva función criptográfica de troceo de los nuevos metadatos, los cuales incluyen ahora el nombre del propietario. Esto hace de forma ventajosa a los metadatos resistentes a manipulación indebida, debido a que cualquier intento de cambiar los metadatos (por ejemplo, eliminar el nombre del propietario legítimo de tal modo que el propietario legítimo podría distribuir las copias y escapar a la detección) daría lugar a que fallara cualquier intento de eliminar el sello de la clave simétrica 14A, debido a que resultaría la función criptográfica de troceo equivocada. No obstante, al igual que con las copias no firmadas y no selladas, y al igual que las copias selladas por la fuente, estos títulos no proporcionan protección pro-activa alguna frente a copia; en su lugar, las copias selladas de forma individual protegen los derechos del propietario en las obras al depender del efecto desalentador de que podría descubrirse con facilidad un usuario cuyo nombre está enlazado a la copia y que se implicó en la distribución ilegal de la copia.

En el escenario, el comerciante minorista en general proporciona el nombre del consumidor, tal como aparece este en su tarjeta de crédito, como un parámetro en cada URL de descarga incluido en el correo electrónico / página de recibo (es decir, de prueba de compra). Esta información es usada por los servidores de descarga 76 durante el cumplimiento para añadir el nombre del usuario a los metadatos. Es preferible el uso del nombre que está asociado con una tarjeta de crédito, debido a que, suponiendo que no se sustraiga la tarjeta de crédito, esta es una fuente fiable del nombre del usuario; si el nombre que es provisto por el comerciante minorista está basado en, póngase por caso, una entrada de usuario, existe un mayor riesgo de que el usuario introdujera un nombre falso que no serviría al fin de enlazar el nombre real del usuario a la copia.

Ventas de copias firmadas

Las copias firmadas (por ejemplo, el nivel 4) son títulos que incluyen una firma digital, la cual fue provista por la fuente de contenido (autor y / o editor) en el momento en el que se generó el título. Este es el mecanismo que se usa para proporcionar copias autenticables, al hacer que los datos en el archivo de LIT (o una porción del mismo) sean firmados por diversas entidades en la cadena de distribución. El nivel 4 se puede combinar con otros niveles - por ejemplo, es posible combinar la firma de fuente con una individualización o bien de nivel 3 o bien de nivel 5 con el fin de crear un título que es tanto autenticable como resistente a copia (o, en el caso del nivel 3, de copia "desalentada").

Ventas de copias completamente individualizadas

Las copias completamente individualizadas difieren de los títulos sellados de forma individual en que en el momento del cumplimiento, el comerciante / distribuidor siempre ha de sellar la licencia mediante el cifrado de la clave simétrica 14A con la clave pública del usuario final en el certificado de activación del usuario final. La autenticidad de la clave pública es avalada por el certificado de activación, el cual es firmado por los servidores de activación 94. Un comerciante puede solicitar el certificado de activación firmado la primera vez que un consumidor particular compre cualquier título completamente individualizado. Opcionalmente, los comerciantes podrían solicitar tal certificado en cada transacción, si el usuario no dispusiera de una pertenencia u otra relación con el comerciante. El certificado de activación cifrado es provisto a un comerciante minorista por un componente de cliente del sistema de DRM, al cual se puede dar como secuencia de comandos por medio de cualquier página web. Este certificado se cifra para proteger la privacidad del consumidor así como reducir el riesgo de ataques de reproducción y / o pirateo. Es preferible que los comerciantes almacenen el certificado de activación cifrado en sus sitios para futuras transacciones.

Los títulos vendidos como copias completamente individualizadas solo se pueden abrir en el lector o lectores del consumidor que realiza la compra y no se puede distribuir abiertamente. Como parte del procedimiento de venta de títulos completamente individualizados, los comerciantes pueden detectar si se ha activado el lector del usuario final, lo cual es un requisito para descargar tales títulos. Si un comerciante detecta que un lector no está activado, el comerciante puede avisar al lector de que es necesaria una activación para abrir un título completamente individualizado. En el caso en el que el comerciante no almacena el certificado de activación de un usuario particular, ni siquiera sería posible proveer un título completamente individualizado para ese usuario. En el caso en el que el comerciante almacena el certificado de activación, el comerciante puede detectar, por ejemplo, que el lector

instalado en el dispositivo del usuario a través del cual el usuario está comprando el título no se ha activado (a pesar de que ese usuario puede tener otros lectores activados), caso en el cual el comerciante puede proporcionar el título al usuario, puede avisar al usuario de que este ha de activar el nuevo dispositivo con el fin de usar el título en ese dispositivo (sujeto, por supuesto, a cualquier límite aplicable sobre las activaciones).

Se hace notar que los ejemplos anteriores se han proporcionado meramente para fines de explicación y no han de interpretarse en modo alguno como limitantes de la presente invención. A pesar de que la invención se ha descrito con referencia a diversas realizaciones, se entiende que las expresiones que se han usado en el presente documento son expresiones de descripción e ilustración, en lugar de expresiones de limitaciones. Además, a pesar de que la invención se ha descrito en el presente documento con referencia a medios, materiales y realizaciones particulares, la invención no tiene por objeto estar limitada a las particularidades que se divulgan en el presente documento, en su lugar, la invención se extiende a todas las estructuras, procedimientos y usos funcionalmente equivalentes, según se encuentren dentro del ámbito de las reivindicaciones adjuntas. Los expertos en la materia, teniendo el beneficio de las enseñanzas de la presente memoria descriptiva, pueden efectuar numerosas modificaciones a la misma y se pueden realizar cambios sin apartarse del ámbito de la invención en sus aspectos.

REIVINDICACIONES

1. Un procedimiento para facilitar la distribución de contenido electrónico por un dispositivo informático de comercio al por menor (71, 72, 74) configurado para proporcionar una funcionalidad para un comerciante minorista de contenido electrónico, comprendiendo dicho procedimiento:

recibir, en el dispositivo informático de comercio al por menor a partir de un dispositivo informático de cliente (90, 92), un pedido de compra para un contenido electrónico;
cifrar, en el dispositivo informático de comercio al por menor, una información que incluye al menos un conjunto de parámetros relativos al contenido electrónico comprado (10), comprendiendo el conjunto de parámetros al menos una identificación del contenido electrónico, estando destinada la información cifrada para un dispositivo informático de contenido (76) configurado para proporcionar el contenido electrónico, siendo el dispositivo informático de contenido diferente del dispositivo informático de cliente y del dispositivo informático de comercio al por menor;
crear, en el dispositivo informático de comercio al por menor, una solicitud de HTTP que incluye una dirección de dicho dispositivo informático de contenido y la información cifrada; y
transmitir dicha solicitud de HTTP desde el dispositivo informático de comercio al por menor al dispositivo informático de cliente, permitiendo que el dispositivo informático de cliente complemente dicha solicitud de HTTP con una porción pública de un par de claves asociado con un comprador asociado con el dispositivo informático de cliente y que inicie una descarga del contenido electrónico a partir del dispositivo informático de contenido usando dicha solicitud de HTTP complementada con dicha porción pública del par de claves, habiéndose emitido el par de claves al comprador para su uso en el dispositivo informático de cliente con la condición de que el comprador presente unas credenciales autenticables y con la condición adicional de que el par de claves no se haya emitido previamente para su uso por el comprador en un número de dispositivos que supere un límite.

2. El procedimiento de la reivindicación 1, en el que dicha información se cifra usando una clave simétrica (75), y en el que dicha clave simétrica es un secreto compartido disponible para dicho dispositivo informático de contenido y no disponible para dicho dispositivo informático de cliente.

3. El procedimiento de la reivindicación 1, que comprende adicionalmente el acto de crear, en el dispositivo informático de comercio al por menor, una página web que incluye un hipervínculo asociado con dicha solicitud de HTTP, en el que dicho acto de transmitir comprende transmitir dicha página web a dicho dispositivo informático de cliente.

4. El procedimiento de la reivindicación 1, en el que la información cifrada incluye una información relativa a la compra de dicho contenido electrónico.

5. El procedimiento de la reivindicación 1, que comprende:

proporcionar, a una primera parte interesada, para su uso en el dispositivo informático de comercio al por menor, un primer conjunto de instrucciones ejecutables por ordenador, el cual realiza el cifrado de la información en base a un id único que establece una correspondencia con un secreto compartido;
proporcionar, a una segunda parte interesada, para su uso en dicho dispositivo informático de contenido (76), un segundo conjunto de instrucciones ejecutables por ordenador, el cual descifra la información cifrada.

6. El procedimiento de la reivindicación 5, en el que dicha primera parte interesada comprende un vendedor del contenido electrónico, en el que dicha segunda parte interesada comprende un proveedor de contenido electrónico vendido por dicha primera parte interesada, y en el que dicha información cifrada se refiere a una transacción entre dicha primera parte interesada y un consumidor de contenido electrónico.

7. El procedimiento de la reivindicación 5, en el que dicho primer conjunto de instrucciones ejecutables por ordenador, comprende un modelo de objetos componentes, COM, (74) que proporciona una funcionalidad para dicho cifrado de dicha información.

8. El procedimiento de la reivindicación 7, en el que dicho primer conjunto de instrucciones ejecutables por ordenador expone un procedimiento de CIFRADO para su uso por un tercer conjunto de instrucciones ejecutables por ordenador el cual se ejecuta en dicho dispositivo informático de comercio al por menor, creando el procedimiento de CIFRADO la información cifrada.

9. El procedimiento de la reivindicación 5, en el que cada uno de dicho dispositivo informático de comercio al por menor y dicho dispositivo informático de contenido puede acceder a, o conoce, una clave simétrica secreta, y en el que dicho primer conjunto de instrucciones ejecutables por ordenador usa dicha clave simétrica secreta para cifrar dicha información.

10. El procedimiento de la reivindicación 2 para construir una solicitud de cliente - servidor, en el que el dispositivo informático de contenido (76) es un servidor, en el que dicha solicitud de cliente - servidor comprende dicha solicitud de HTTP, y en el que crear la solicitud de HTTP comprende:

incluir dicha dirección asociada con dicho primer servidor en dicha solicitud de HTTP; e
incluir la información cifrada en dicha solicitud de HTTP.

11. El procedimiento de la reivindicación 10, en el que la información cifrada incluye una información relativa a una transacción para comprar dicho contenido electrónico, en el que dicho servidor promueve al menos un cierto aspecto de dicha transacción.

12. El procedimiento de una de las reivindicaciones 4, 5 y 11, en el que la información cifrada incluye una información (14c) la cual identifica a dicho comprador de dicho contenido electrónico.

13. El procedimiento de la reivindicación 10, en el que dicha información se cifra usando un secreto que comprende una clave simétrica (75), y en el que la información cifrada se genera mediante el cifrado de una información de texto no cifrado con dicha clave simétrica.

14. El procedimiento de la reivindicación 1
en el que dicha dirección de dicho dispositivo informático de contenido es una dirección de red del dispositivo informático de contenido; y
en el que dicho dispositivo informático de contenido procesa dicho pedido mediante el uso de al menos parte de dicha información cifrada.

15. El procedimiento de la reivindicación 14, en el que dicha información cifrada incluye una información (14c) que identifica al individuo que emitió dicho pedido.

16. El procedimiento de la reivindicación 14, en el que dicho contenido electrónico no reside en dicho dispositivo informático de comercio al por menor.

17. El procedimiento de la reivindicación 1, que comprende:

recibir el conjunto de parámetros que identifican características de una primera transacción entre el dispositivo informático de cliente y el dispositivo informático de comercio al por menor que es un primer servidor;
en el que transmitir comprende devolver dichos parámetros cifrados a dicho dispositivo informático de cliente en un formato de tal modo que el dispositivo informático de contenido, que es un segundo servidor, pueda recibir dicha información cifrada de dicho dispositivo informático de cliente, validar dicha primera transacción e iniciar una segunda transacción sin interacción alguna con dicho primer servidor.

18. El procedimiento de la reivindicación 17, en el que dicho primer servidor ha implementado un modelo de objetos componentes, COM, (74) que proporciona una funcionalidad para dicho cifrado de dicha información.

19. El procedimiento de la reivindicación 17, en el que dicha primera transacción se refiere a la compra del contenido electrónico.

20. El procedimiento de la reivindicación 19, en el que dicha segunda transacción comprende la descarga de dicho contenido electrónico.

21. El procedimiento de la reivindicación 19, en el que dichos parámetros comprenden una información de usuario final que posibilita la individualización de dicho contenido electrónico.

22. El procedimiento de la reivindicación 17, en el que dichos parámetros incluyen adicionalmente una información que identifica una parte interesada de dicha primera transacción.

23. El procedimiento de una de las reivindicaciones 1, 11, 14 y 17, que comprende adicionalmente:

incluir una marca de tiempo en dicha información cifrada.

24. El procedimiento de una de las reivindicaciones 1, 14 y 17, que comprende adicionalmente los actos de:

computar una función de troceo de dicha información antes del cifrado; e
incluir dicha función de troceo en dicha solicitud de HTTP.

25. El procedimiento de la reivindicación 24, en el que dicha función de troceo se computa usando un algoritmo SHA1.

26. El procedimiento de la reivindicación 17, en el que dicho acto de cifrado comprende aplicar una clave simétrica secreta compartida entre dicho primer servidor y dicho segundo servidor.

27. El procedimiento de la reivindicación 1, en el que el cifrado comprende cifrar la información de tal modo que la información cifrada sea descifrable por un secreto, siendo transmisible dicha información cifrada a dicho dispositivo informático de contenido tras la instrucción procedente de un usuario que opera dicho dispositivo informático de cliente, en el que o bien dicho dispositivo informático de cliente o bien dicho usuario no puede acceder a dicho secreto; y en el que el procedimiento comprende el acto de:

compartir dicho secreto mediante la realización de uno cualquiera de los siguientes actos:

proporcionar dicho secreto a dicho dispositivo informático de contenido o a una parte interesada asociada con dicho dispositivo informático de contenido; o
recibir dicho secreto desde dicho dispositivo informático de contenido o desde una parte interesada asociada con dicho dispositivo informático de contenido.

28. El procedimiento de la reivindicación 27, en el que la información cifrada incluye una información relativa a la compra de dicho contenido.

29. El procedimiento de la reivindicación 27, en el que dicho acto de transmisión comprende transmitir la información cifrada a través de una red de área extensa.

30. El procedimiento de la reivindicación 29, en el que dicha red de área extensa comprende Internet.

31. El procedimiento de una de las reivindicaciones 1, 5, 10, 14 y 27, en el que dicha solicitud de HTTP comprende una solicitud de POST, y en el que dicha información cifrada está incluida en el cuerpo de dicha solicitud de POST.

32. El procedimiento de una de las reivindicaciones 1, 5, 10, 14 y 27, en el que dicha solicitud de HTTP comprende una solicitud de GET, y en el que dicha información cifrada está anexada a dicha solicitud de GET como un parámetro.

33. El procedimiento de la reivindicación 27, que comprende adicionalmente el acto de crear una página web que incluye un vínculo asociado con dicha solicitud de HTTP, en el que dicho acto de transmisión comprende transmitir dicha página web a dicho dispositivo informático de cliente, y en el que la instrucción del usuario para transmitir la información cifrada a dicho dispositivo informático de contenido comprende que el usuario use un dispositivo de entrada asociado con dicho dispositivo informático de cliente para accionar dicho vínculo.

34. El procedimiento de la reivindicación 27, en el que dicho secreto comprende una clave simétrica, y en el que dicho acto de cifrado comprende cifrar dicha información con dicha clave simétrica.

35. El procedimiento de la reivindicación 27, que comprende adicionalmente el acto de incluir una marca de tiempo en la información cifrada.

36. El procedimiento de la reivindicación 27, que comprende adicionalmente el acto de anexar una función de troceo de dicha información a dicha información cifrada, computándose dicha función de troceo antes del cifrado de dicha información.

37. Un medio legible por ordenador que tiene unas instrucciones ejecutables por ordenador para realizar el procedimiento de una de las reivindicaciones 1 a 36.

FIG. 1

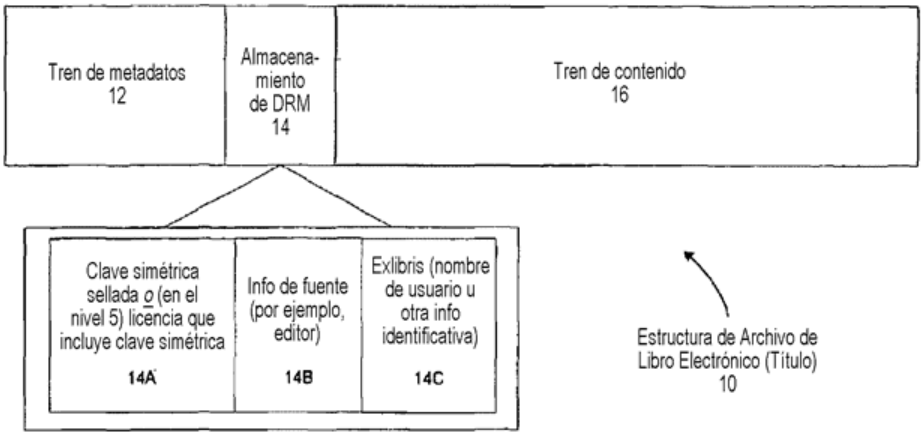
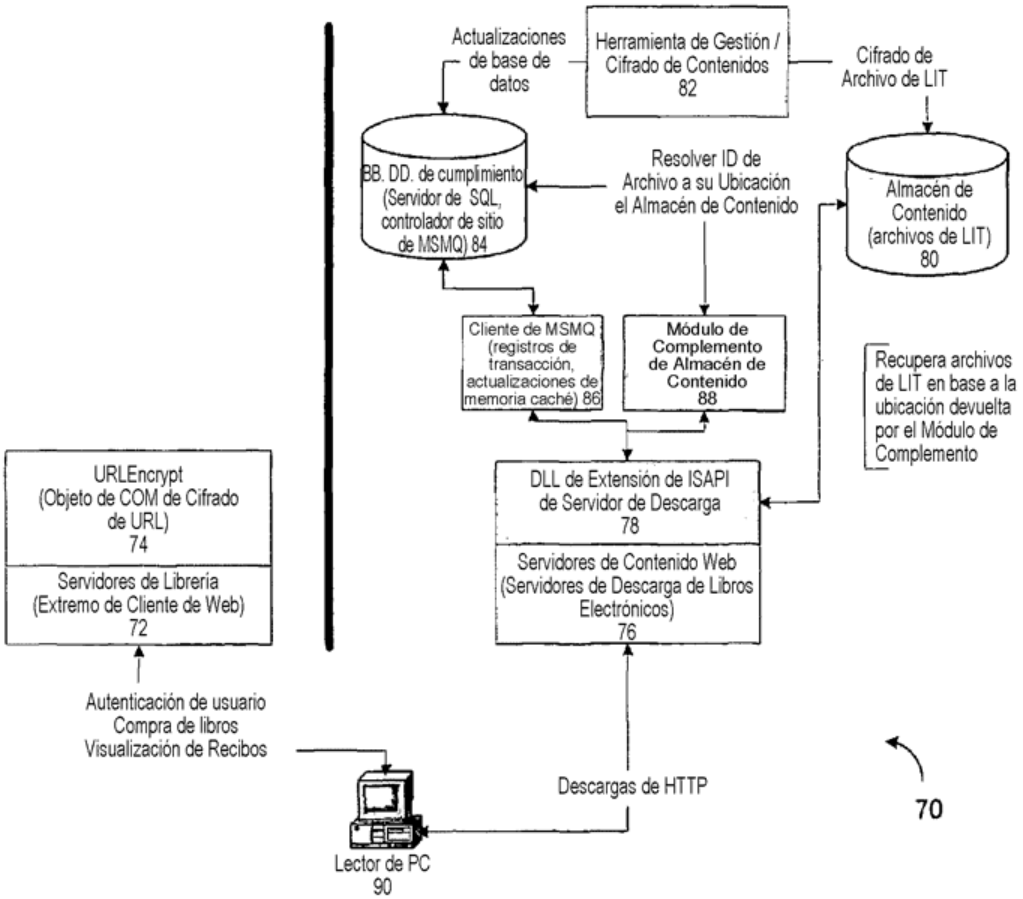

Tren de metadatos
12
Almacena-
miento
de DRM
14
Tren de contenido
16
Clave simétrica
sellada o (en el
nivel 5) licencia que
incluye clave simétrica
14A
Info de fuente
(por ejemplo,
editor)
14B
Exlibris (nombre
de usuario u
otra info
identificativa)
14C
Estructura de Archivo de
Libro Electrónico (Título)
10

FIG. 3


Actualizaciones
de base de
datos
Herramienta de Gestión /
Cifrado de Contenidos
82
Cifrado de
Archivo de LIT
BB. DD. de cumplimiento
(Servidor de SQL,
controlador de sitio
de MSMQ) 84
Resolver ID de
Archivo a su Ubicación
el Almacén de Contenido
Almacén de
Contenido
(archivos de LIT)
80
Cliente de MSMQ
(registros de
transacción,
actualizaciones de
memoria caché) 86
Módulo de
Complemento
de Almacén de
Contenido
88
Recupera archivos
de LIT en base a la
ubicación devuelta
por el Módulo de
Complemento
URLEncrypt
(Objeto de COM de Cifrado
de URL)
74
Servidores de Librería
(Extremo de Cliente de Web)
72
DLL de Extensión de ISAPI
de Servidor de Descarga
78
Servidores de Contenido Web
(Servidores de Descarga de Libros
Electrónicos)
76
Autenticación de usuario
Compra de libros
Visualización de Recibos
Descargas de HTTP
70
Lector de PC
90

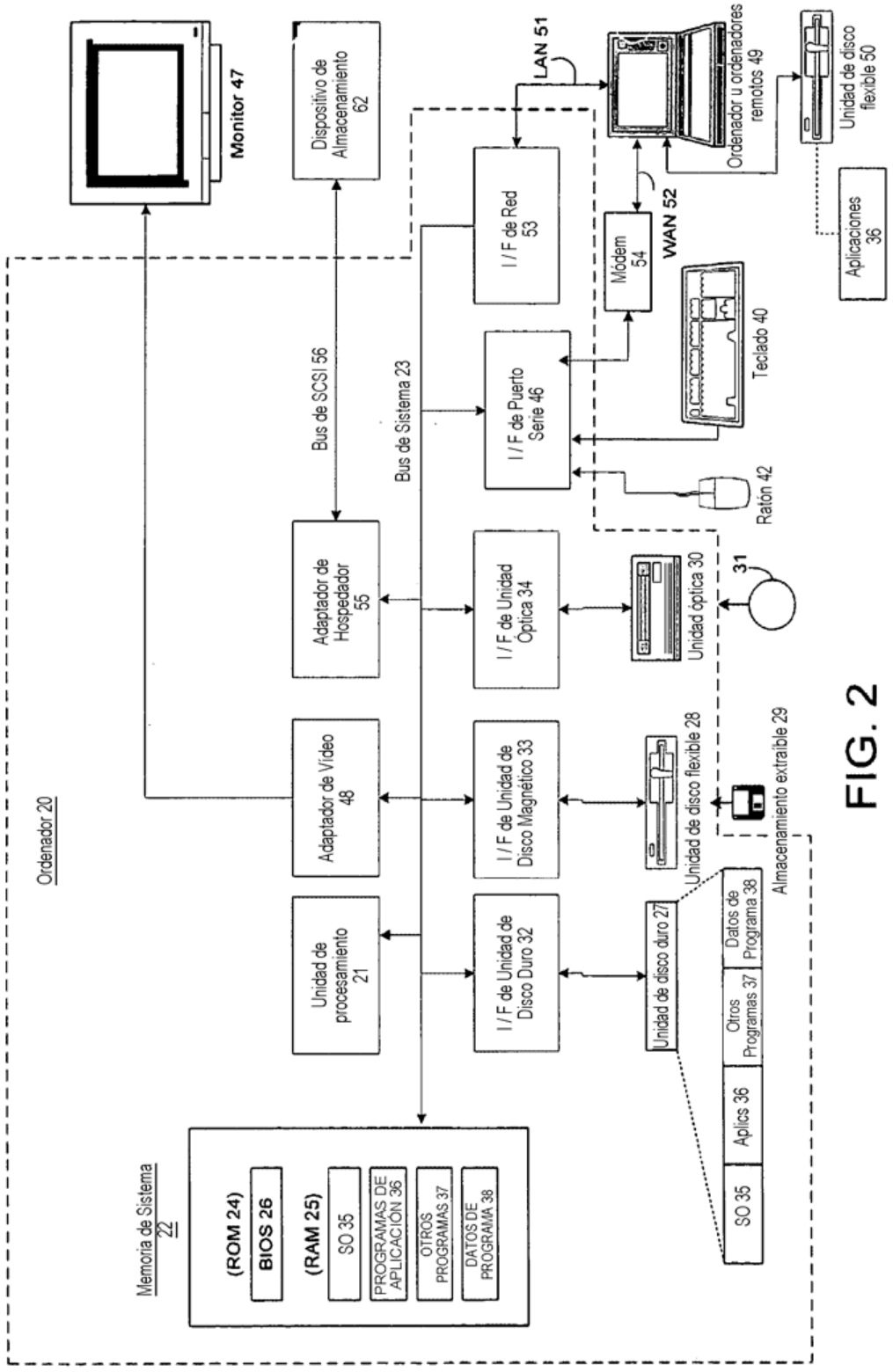

Ordenador 20
Monitor 47
Dispositivo de Almacenamiento 62
LAN 51
Ordenador u ordenadores remotos 49
Unidad de disco flexible 50
Aplicaciones 36
WAN 52
Módem 54
I / F de Red 53
Teclado 40
Ratón 42
I / F de Puerto Serie 46
Bus de SCSI 56
Bus de Sistema 23
Adaptador de Hospedador 55
I / F de Unidad Óptica 34
Unidad óptica 30
31
Adaptador de Vídeo 48
I / F de Unidad de Disco Magnético 33
Unidad de disco flexible 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
Aplics 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. 2

FIG. 4

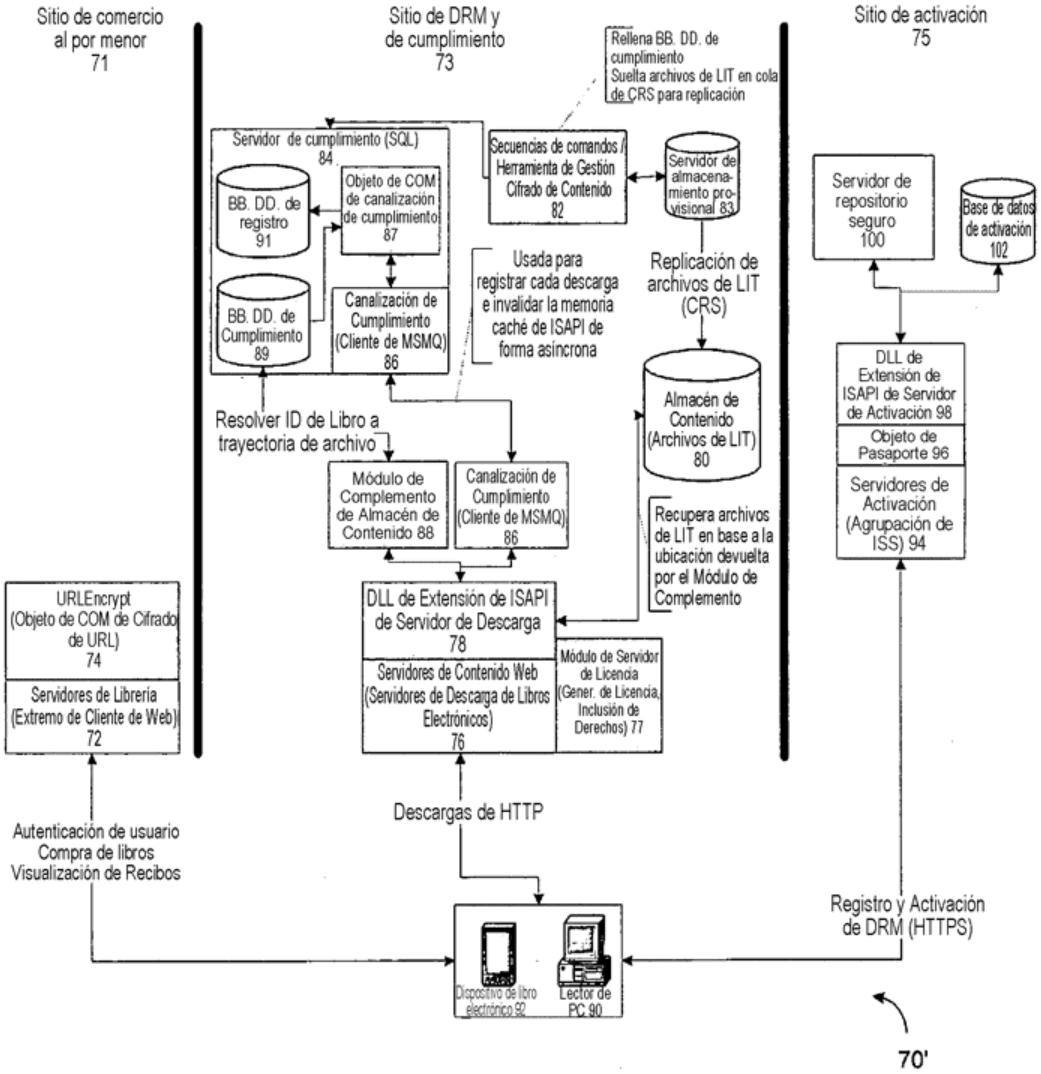

Sitio de comercio al por menor 71
Sitio de DRM y de cumplimiento 73
Sitio de activación 75
Rellena BB. DD. de cumplimiento
Suelta archivos de LIT en cola de CRS para replicación
Servidor de cumplimiento (SQL) 84
BB. DD. de registro 91
Objeto de COM de canalización de cumplimiento 87
BB. DD. de Cumplimiento 89
Canalización de Cumplimiento (Cliente de MSMQ) 86
Secuencias de comandos / Herramienta de Gestión Cifrado de Contenido 82
Servidor de almacenamiento provisional 83
Usada para registrar cada descarga e invalidar la memoria caché de ISAPI de forma asíncrona
Replicación de archivos de LIT (CRS)
Servidor de repositorio seguro 100
Base de datos de activación 102
DLL de Extensión de ISAPI de Servidor de Activación 98
Objeto de Pasaporte 96
Servidores de Activación (Agrupación de ISS) 94
Almacén de Contenido (Archivos de LIT) 80
Resolver ID de Libro a trayectoria de archivo
Módulo de Complemento de Almacén de Contenido 88
Canalización de Cumplimiento (Cliente de MSMQ) 86
Recupera archivos de LIT en base a la ubicación devuelta por el Módulo de Complemento
URLEncrypt (Objeto de COM de Cifrado de URL) 74
Servidores de Librería (Extremo de Cliente de Web) 72
DLL de Extensión de ISAPI de Servidor de Descarga 78
Servidores de Contenido Web (Servidores de Descarga de Libros Electrónicos) 76
Módulo de Servidor de Licencia (Gener. de Licencia, Inclusión de Derechos) 77
Descargas de HTTP
Autenticación de usuario
Compra de libros
Visualización de Recibos
Registro y Activación de DRM (HTTPS)
Dispositivo de libro electrónico 92
Lector de PC 90
70'

FIG. 5

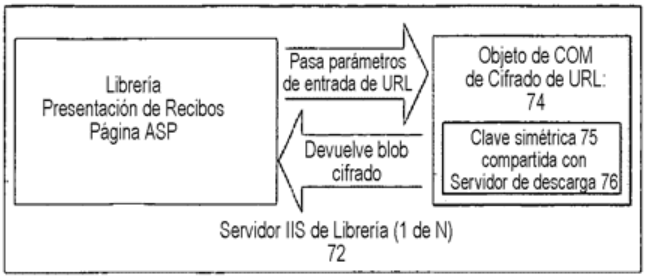

Librería
Presentación de Recibos
Página ASP
Pasa parámetros de entrada de URL
Devuelve blob cifrado
Objeto de COM de Cifrado de URL: 74
Clave simétrica 75 compartida con Servidor de descarga 76
Servidor IIS de Librería (1 de N) 72

FIG. 6

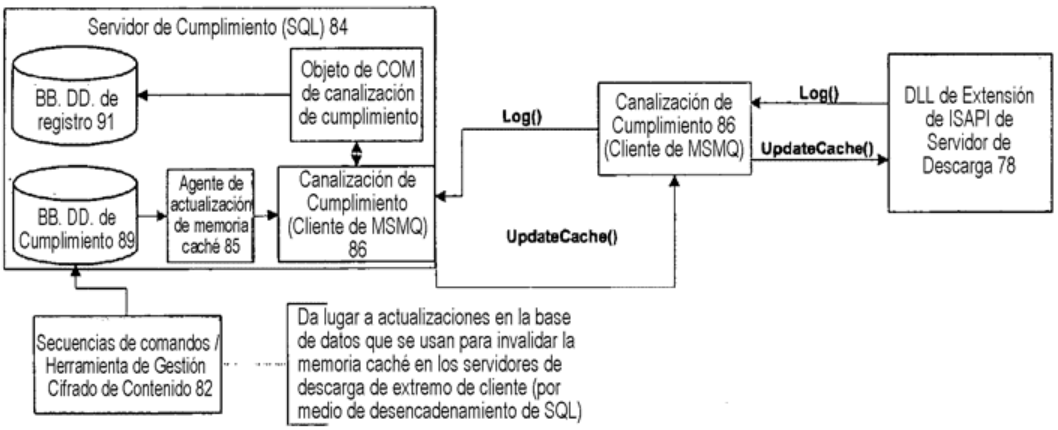

Servidor de Cumplimiento (SQL) 84
BB. DD. de registro 91
Objeto de COM de canalización de cumplimiento
BB. DD. de Cumplimiento 89
Agente de actualización de memoria caché 85
Canalización de Cumplimiento (Cliente de MSMQ) 86
Log()
UpdateCache()
Canalización de Cumplimiento 86 (Cliente de MSMQ)
Log()
UpdateCache()
DLL de Extensión de ISAPI de Servidor de Descarga 78
Secuencias de comandos / Herramienta de Gestión Cifrado de Contenido 82
Da lugar a actualizaciones en la base de datos que se usan para invalidar la memoria caché en los servidores de descarga de extremo de cliente (por medio de desencadenamiento de SQL)

FIG. 7

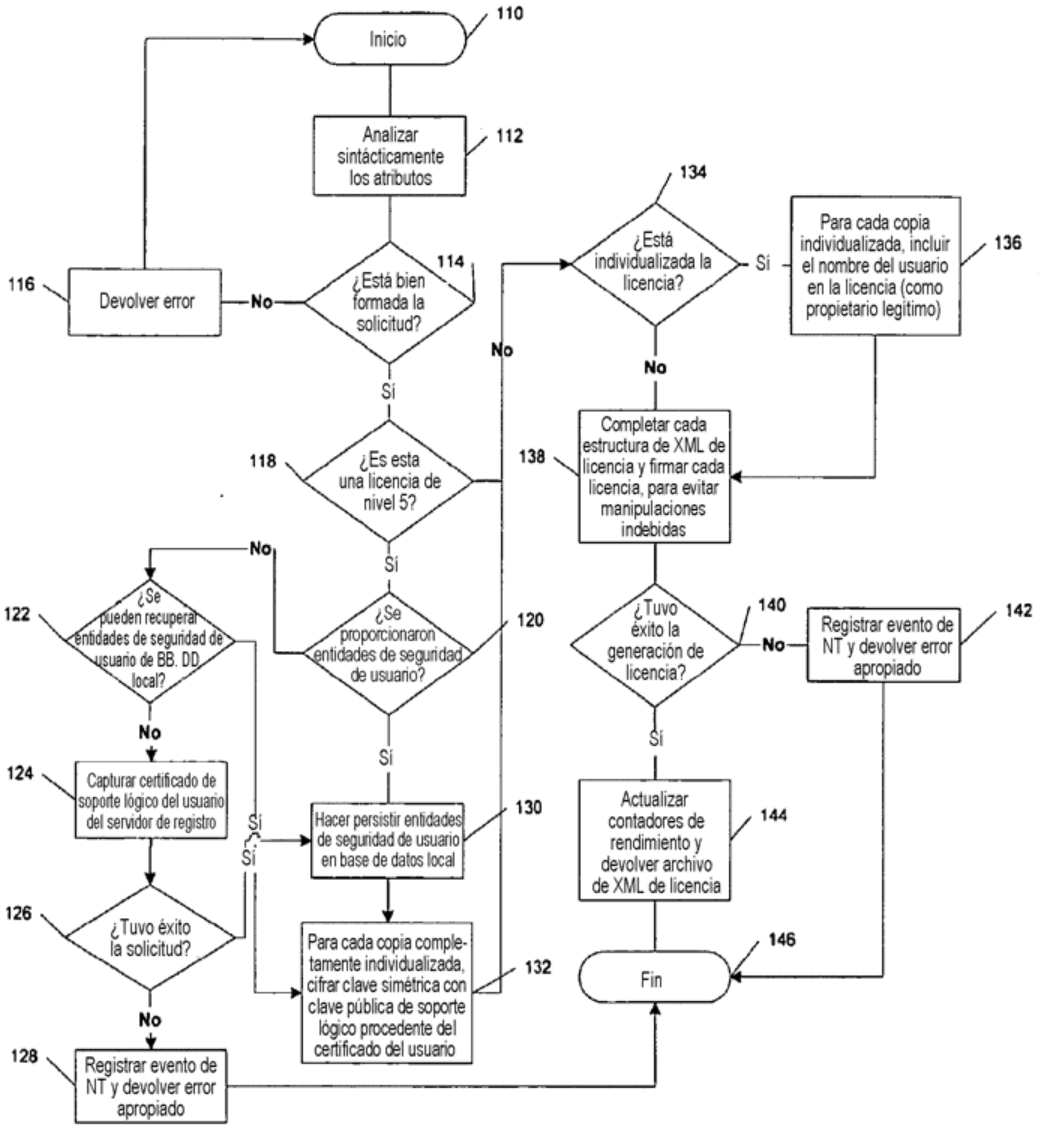

Inicio
110
Analizar sintácticamente los atributos
112
¿Está bien formada la solicitud?
114
Devolver error
116
No
Sí
¿Es esta una licencia de nivel 5?
118
No
Sí
¿Se proporcionaron entidades de seguridad de usuario?
120
No
Sí
¿Se pueden recuperar entidades de seguridad de usuario de BB. DD. local?
122
No
Capturar certificado de soporte lógico del usuario del servidor de registro
124
¿Tuvo éxito la solicitud?
126
No
Registrar evento de NT y devolver error apropiado
128
Hacer persistir entidades de seguridad de usuario en base de datos local
130
Para cada copia completamente individualizada, cifrar clave simétrica con clave pública de soporte lógico procedente del certificado del usuario
132
¿Está individualizada la licencia?
134
Sí
Para cada copia individualizada, incluir el nombre del usuario en la licencia (como propietario legítimo)
136
No
Completar cada estructura de XML de licencia y firmar cada licencia, para evitar manipulaciones indebidas
138
¿Tuvo éxito la generación de licencia?
140
No
Registrar evento de NT y devolver error apropiado
142
Sí
Actualizar contadores de rendimiento y devolver archivo de XML de licencia
144
Fin
146

FIG. 8

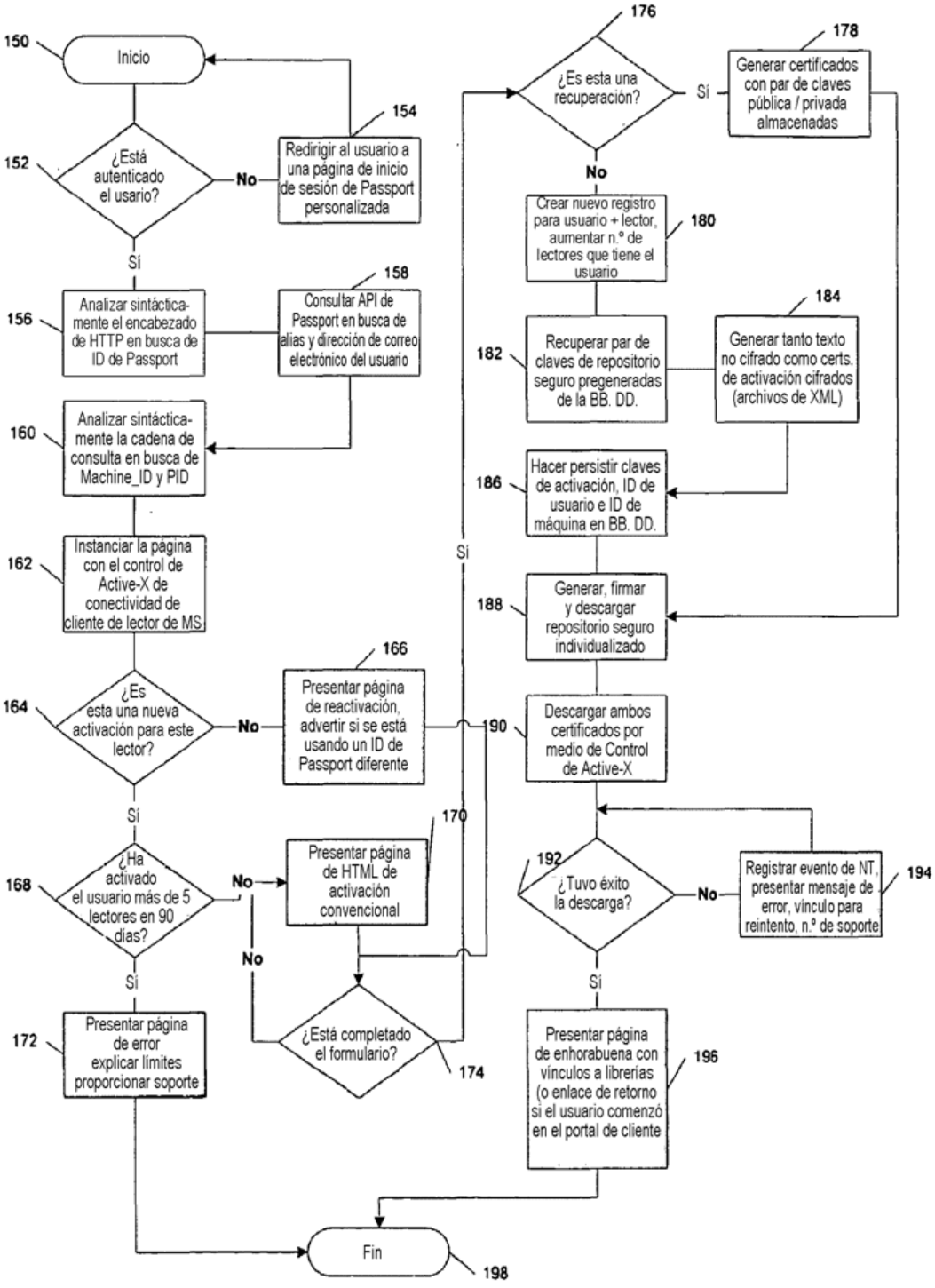

150
Inicio
152
¿Está autenticado el usario?
No
154
Redirigir al usuario a una página de inicio de sesión de Passport personalizada
Sí
156
Analizar sintáctica-mente el encabezado de HTTP en busca de ID de Passport
158
Consultar API de Passport en busca de alias y dirección de correo electrónico del usuario
160
Analizar sintáctica-mente la cadena de consulta en busca de Machine_ID y PID
162
Instanciar la página con el 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 reactivación, advertir si se está usando un 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 soporte
No
¿Está completado el formulario?
174
Sí
176
¿Es esta una recuperación?
Sí
178
Generar certificados con par de claves pública / privada almacenadas
No
180
Crear nuevo registro para usuario + lector, aumentar n.º de lectores que tiene el usuario
182
Recuperar par de claves de repositorio seguro pregeneradas de la BB. DD.
184
Generar tanto texto no cifrado como certs. de activación cifrados (archivos de XML)
186
Hacer persistir claves de activación, ID de usuario e ID de máquina en BB. DD.
188
Generar, firmar y descargar repositorio seguro individualizado
190
Descargar ambos certificados por medio de Control de Active-X
192
¿Tuvo éxito la descarga?
No
194
Registrar evento de NT, presentar mensaje de error, vínculo para reintento, n.º de soporte
Sí
196
Presentar página de enhorabuena con vínculos a librerías (o enlace de retorno si el usuario comenzó en el portal de cliente
Fin
198

FIG. 9

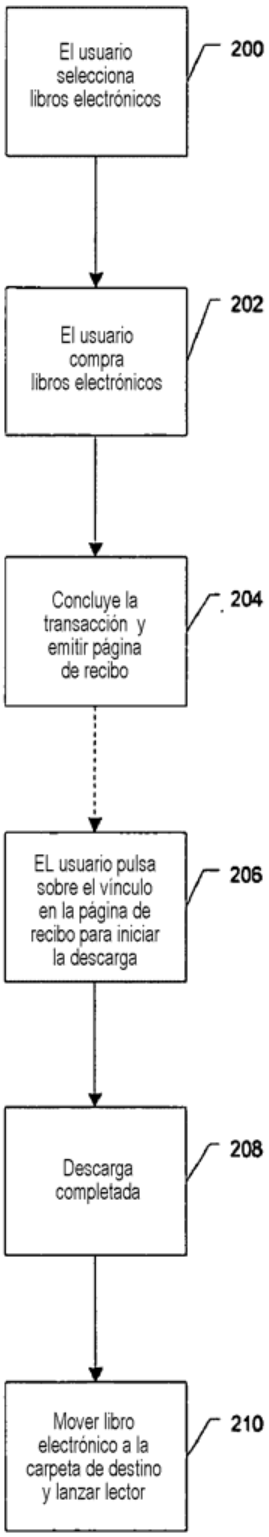
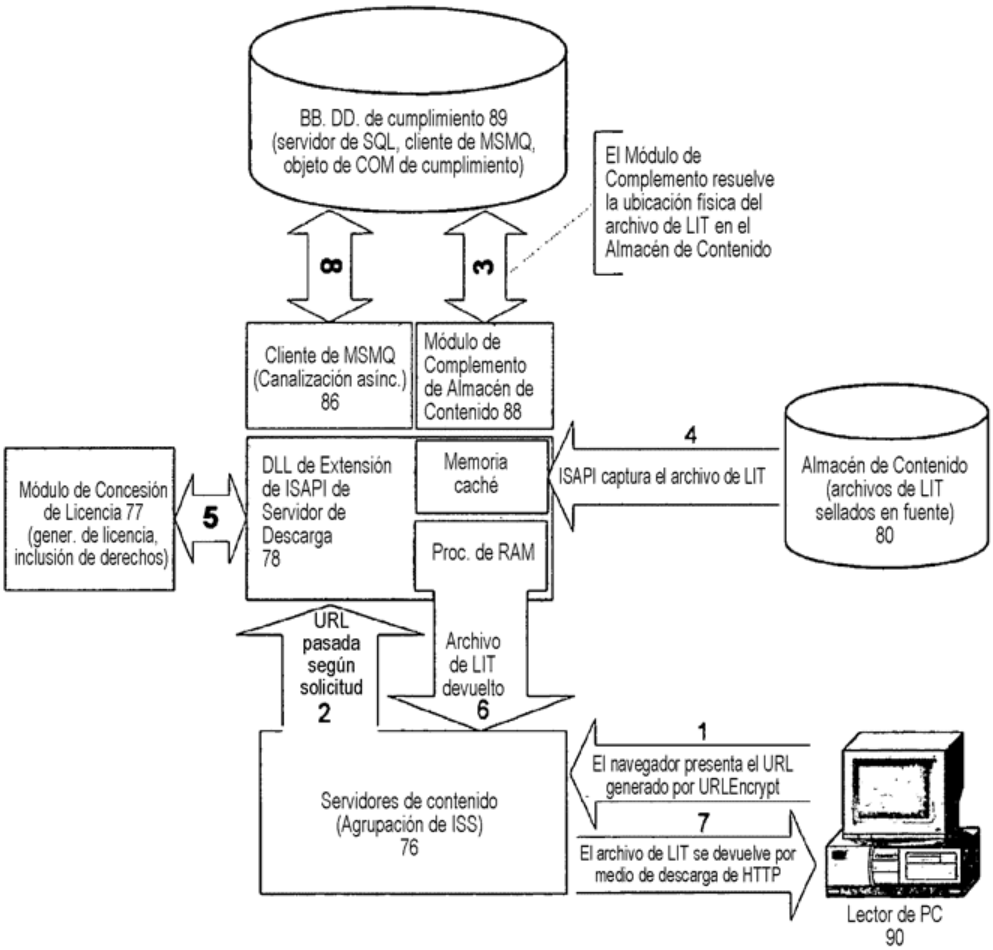

El usuario selecciona libros electrónicos
200
El usuario compra libros electrónicos
202
Concluye la transacción y emitir página de recibo
204
EL usuario pulsa sobre el vínculo en la página de recibo para iniciar la descarga
206
Descarga completada
208
Mover libro electrónico a la carpeta de destino y lanzar lector
210

FIG. 10


BB. DD. de cumplimiento 89
(servidor de SQL, cliente de MSMQ, objeto de COM de cumplimiento)
El Módulo de Complemento resuelve la ubicación física del archivo de LIT en el Almacén de Contenido
8
3
Cliente de MSMQ (Canalización asínc.) 86
Módulo de Complemento de Almacén de Contenido 88
4
Módulo de Concesión de Licencia 77 (gener. de licencia, inclusión de derechos)
5
DLL de Extensión de ISAPI de Servidor de Descarga 78
Memoria caché
ISAPI captura el archivo de LIT
Almacén de Contenido (archivos de LIT sellados en fuente) 80
Proc. de RAM
URL pasada según solicitud 2
Archivo de LIT devuelto 6
1
El navegador presenta el URL generado por URLEncrypt
7
El archivo de LIT se devuelve por medio de descarga de HTTP
Servidores de contenido (Agrupación de ISS) 76
Lector de PC 90