(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 592 903**

(51) Int. CI.:

G06F 21/10 (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **13.12.2000 PCT/US2000/33727**

(87) Fecha y número de publicación internacional: **21.06.2001 WO0144908**

(96) Fecha de presentación y número de la solicitud europea: **13.12.2000 E 00986345 (7)**

(97) Fecha y número de publicación de la concesión europea: **22.06.2016 EP 1242855**

(54) Título: **Servidor para un sistema de distribución electrónico y procedimiento de operación del mismo**

(30) Prioridad:

17.12.1999 US 172318 P
17.12.1999 US 172319 P
27.06.2000 US 604540

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
02.12.2016

(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

Servidor para un sistema de distribución electrónico y procedimiento de operación del mismo

Referencia cruzada a casos relacionados

Esta solicitud reivindica el beneficio de la Solicitud Provisional de Estados Unidos N.º 60/172.318 titulada “System for Distributing Content Having Multinivel Security Protection” y de la Solicitud Provisional de Estados Unidos N.º 60/172.319 titulada “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 particularmente al uso de un servidor para distribuir contenido de acuerdo con un sistema de gestión de derechos digitales.

Antecedentes de la invención

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

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

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

El documento WO 96/42041 se refiere al procesamiento de solicitudes de servicio desde un cliente a un servidor a través de una red. Un cliente dirige una solicitud de servicio a un primer servidor que comprueba si la solicitud de servicio requiere un identificador de sesión. Si es así, el primer servidor redirige la solicitud de servicio desde el cliente a un servidor de autorización que expide un identificador de sesión para anexarse a la solicitud de servicio. El cliente recibe y reenvía la solicitud de servicio anexada con el identificador de sesión al primer servidor. Finalmente, el primer servidor reconoce el identificador de sesión y da servicio a la solicitud para el cliente.

Sumario de la invención

Es el objeto de la invención proporcionar un procedimiento y sistema simplificados para proporcionar contenido electrónico.

Este objeto se resuelve mediante la invención como se reivindica en las reivindicaciones independientes.

Se definen realizaciones preferidas en las reivindicaciones dependientes.

Se proporciona una arquitectura de servidor que soporta la distribución de contenido protegido en un sistema de gestión de derechos digitales (“DRM”). 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 distribución no autorizada o uso de contenido protegido, así como componentes de software que

implementan las características de seguridad.

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

La disposición de servidor de activación incluye uno o más dispositivos de computación de servidor que "activan" dispositivos de computación de cliente proporcionando código y datos a estos dispositivos, donde el código y los datos son necesarios para acceder a 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 encriptada, y el "código" es un programa (por ejemplo, un "repositorio seguro") que accede a la clave privada en el certificado de activación aplicando, de una manera segura, la clave necesaria para desencriptar la clave privada encriptada. Preferentemente, el par de claves en el certificado de activación está asociado de manera persistente con una "persona" autenticable, de manera que un dispositivo puede "activarse" para leer contenido que se ha individualizado para esa persona, pero no contenido que se ha "individualizado completamente" para otras personas. Como se usa en el presente documento, una "persona" es un identificador único que puede vincularse a un usuario y puede autenticarse de manera segura mediante un procedimiento fuera de banda - por ejemplo, una forma de nombre de usuario y contraseña en un explorador web para uso a través de una capa de conexión segura (SSL) es una realización de ejemplo de un procedimiento de este tipo. Además, la disposición de servidor de activación preferentemente proporciona un certificado de activación dado (es decir, un certificado de activación que tiene un par de claves particular) únicamente después de autenticar los credenciales (por ejemplo, un nombre de usuario y contraseña) asociados con una persona. De acuerdo con una característica de la invención, el número de dispositivos que una persona particular puede activar puede limitarse por porcentaje y/o por número (por ejemplo, cinco activaciones en un primer periodo de 90 días, seguido por una activación adicional cada periodo de 90 días posterior, hasta un máximo de diez activaciones), evitando de esta manera la proliferación no comprobada de dispositivos en los que puede presentarse contenido individualizado. Como un ejemplo de uso de esta técnica, el contenido protegido puede distribuirse como un fichero que incluye contenido encriptado con una clave simétrica, donde la propia clave simétrica se proporciona mediante una construcción de licencia embebida en el fichero en una forma encriptada mediante la clave pública del certificado, haciendo por lo tanto necesario tener tanto el certificado de activación como el repositorio seguro acompañante antes de interconectar con el contenido con licencia.

La disposición de servidor de distribución incluye uno o más servidores de venta minorista y uno o más sitios de ejecución. Los servidores de venta minorista venden contenido protegido (o designan de otra manera a los usuarios para recibir contenido protegido). Los sitios de ejecución proporcionan el contenido real que se ha vendido mediante los servidores de venta minorista. El operador de un servidor de venta minorista puede ser una entidad diferente del operador de un sitio de ejecución, haciendo de esta manera posible para un vendedor minorista vender contenido protegido simplemente firmando un acuerdo en el cual un sitio de ejecución proporcionará contenido vendido por el vendedor minorista. Esto permite al vendedor minorista vender contenido sin invertir en los medios para almacenar o distribuir el contenido. En un ejemplo, el vendedor minorista y el sitio de ejecución acuerdan un secreto (por ejemplo, una clave criptográfica), y el vendedor minorista equipa su servidor con software que usa el secreto para crear una instrucción encriptada para proporcionar el contenido al comprador. El vendedor minorista puede a continuación permitir al comprador "ejecutar" su compra proporcionando una solicitud de HTTP al comprador (por ejemplo, una solicitud de POST presentada como un hiperenlace en una página web de "recibo" o de "confirmación"), donde la solicitud de HTTP contiene la dirección del sitio de ejecución y la instrucción encriptada. En el caso de que el contenido requiera algún nivel de individualización, la instrucción encriptada puede incluir la información de individualización (por ejemplo, el nombre del comprador, o, en el caso de contenido "completamente individualizado", el certificado de activación del comprador). El sitio de ejecución recibe la instrucción encriptada cuando el comprador hace clic en el enlace, y el sitio de ejecución usa el secreto compartido para desencriptar la instrucción y proporcionar el contenido de acuerdo con ello. Un objeto de modelo de objetos de componente (COM) puede proporcionarse al vendedor minorista que crea la instrucción encriptada.

El sitio de ejecución puede organizarse como un servidor de ejecución más uno o más servidores de “descarga” y un almacenamiento de contenido. El almacenamiento de contenido almacena contenido a distribuirse a los consumidores. El servidor de ejecución mantiene bases de datos de información relacionadas con la ejecución de pedidos de contenido, tal como la localización física de elementos de contenido y el secreto (por ejemplo, la clave criptográfica) necesario para desencriptar instrucciones recibidas desde el vendedor minorista. Los servidores de descarga realizan la descarga real de contenido a los consumidores/compradores del contenido, así como cualquier preparación del contenido que es necesaria para cumplir los requisitos de protección asociados con el contenido (por ejemplo, el servidor de descarga puede realizar la individualización del contenido). Cada servidor de descarga puede tener una caché, donde el servidor de descarga obtiene una copia de un elemento de contenido desde el almacenamiento de contenido (de acuerdo con la localización especificada en la base de datos del servidor ejecución) la primera vez que se pide al servidor de descarga tras procesar una descarga de ese elemento, donde el servidor de descarga almacena el elemento en la caché para futuras descargas. La caché puede tener límites asociados con la misma, y puede hacer expirar elementos fuera de la caché basándose en un algoritmo tal como un algoritmo de “menos recientemente usado”. El servidor de descarga puede proporcionar también información con respecto a las descargas que procesa al servidor de ejecución para entrada en un registro. El servidor de descarga puede proporcionar esta información en forma de mensajes a través de una mensajería asíncrona, tal como MICROSOFT MESSAGE QUEUE (MSMQ). El servidor de ejecución puede almacenar la información en una “base de datos de registro”. Adicionalmente, cuando se realizan actualizaciones a la información almacenada en el servidor de ejecución que afectan al elemento de contenido almacenado en la caché, el servidor de ejecución puede usar el servicio de mensajería para enviar mensajes a los diversos servidores de descarga que indican que el elemento debería invalidarse en las cachés del servidor de descarga.

Otras características de la invención se describen a continuación.

Breve descripción de los dibujos

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

La Figura 1 es un formato de fichero de título de libro electrónico (eBook) ejemplar;
La Figura 2 es un diagrama de bloques que muestra un entorno de computación ejemplar en el que pueden implementarse los aspectos de la presente invención;
La Figura 3 es un diagrama de bloques de una realización de una primera arquitectura de servidor que implementa 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 aspectos de un sistema de gestión de derechos digitales de acuerdo con la invención;
La Figura 5 es un diagrama de bloques que ilustra ciertas interacciones dentro de un servidor de proveedor de contenido de acuerdo con aspectos de la invención;
La Figura 6 es un diagrama de bloques que muestra componentes de una tubería de ejecución asíncrona de acuerdo con aspectos de la invención;
La Figura 7 es un diagrama de flujo que ilustra el procedimiento para generar una licencia de acuerdo con 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 aspectos de la invención; y
Las Figuras 9 y 10 son diagramas de bloques que ilustran un flujo de comercio electrónico de acuerdo con aspectos de la invención.

Descripción detallada de la invención

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

Vista general

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

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

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

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

El siguiente nivel de protección ("Nivel 4") es "firmado de origen". Los libros electrónicos firmados de origen son títulos que pueden autenticarse por un "lector" (que, como se analiza más particularmente a continuación, es una aplicación de usuario que posibilita la lectura de libros electrónicos en un dispositivo de computación, tal como un PC, un portátil, un Asistente Digital Personal (PDA), PocketPC, o un dispositivo de lectura construido para tal fin). La autenticidad puede definirse preferentemente en tres diversidades: "herramienta firmada", que garantiza que el título de libro electrónico se generó por una conversión confiable y herramienta de encriptación; "propietario firmado" que es un libro electrónico de herramienta firmada que también garantiza la autenticidad del contenido en la copia (por ejemplo, el propietario puede ser el autor u otro titular de los derechos de autor); y "proveedor firmado", que es un libro electrónico de herramienta firmada que confirma a la autenticidad de su proveedor (por ejemplo, el editor o vendedor minorista del contenido). La "herramienta", el propietario y el proveedor puede tener cada uno su propio par de claves asimétricas para facilitar la creación y validación de firmas digitales de la información. Un título puede estar tanto firmado de proveedor como firmado de origen, que facilita la autenticación del canal de distribución del título (por ejemplo, a través de una cadena de firma en la copia). El nivel más fuerte de protección es "completamente individualizado" o "exclusivo de propietario" ("Nivel 5"). Los títulos "completamente individualizados" únicamente pueden abrirse mediante aplicaciones de lector autenticadas que están "activadas" para un usuario particular, protegiendo de esta manera contra la portabilidad de un título de un lector (o lectores) de una persona a un lector que no está registrado para esa persona. Para que el lector de la presente invención abra un título protegido en el Nivel 5, el lector debe estar "activado" (es decir, el dispositivo en el que el reside el lector debe tener un certificado de activación para una persona particular, y un repositorio seguro). El procedimiento de activación se describe en mayor detalle a continuación con referencia a la Figura 8.

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

Estructura de ficheros de libro electrónico

El sistema de DRM de la presente invención protege contenido incorporándolo en una estructura de ficheros, tal como la estructura ejemplar mostrada en la Figura 1. Haciendo referencia a la Figura 1, el libro electrónico contiene contenido 16, que es texto tal como un libro (o cualquier contenido electrónico) que se haya encriptado mediante una clave (la "clave de contenido"), que ella misma ha sido encriptada y/o sellada. En una realización preferida, la clave es una clave 14A simétrica que está sellada con un troceo criptográfico de metadatos 12 o, en el caso de los títulos del nivel 5, con la clave pública del certificado de activación del usuario. Esta clave se almacena como un flujo separado en una sección de sub-almacenamiento del fichero de libro electrónico (almacenamiento 14 de DRM en el diagrama) o, en el caso de títulos de nivel 5, en la licencia. (En el caso de títulos de nivel 5, en lugar de almacenar la clave de contenido como un flujo separado, el flujo 14A contiene una licencia, que es una construcción que define los derechos que el usuario puede ejercer tras la compra del título. En títulos que tienen una licencia, la clave de contenido está contenida en la licencia). También incluido en el almacenamiento 14 de DRM está el flujo 14B de origen, que puede incluir el nombre del editor (u otro origen de contenido), así como el flujo 14C exlibris, que, para títulos sellados individualmente (nivel 3 y/o nivel 5), incluye el nombre del consumidor según se proporciona mediante el vendedor minorista (que puede obtenerse, por ejemplo, como parte de la transacción comercial de compra de un libro electrónico 10, tal como desde la información de la tarjeta de crédito del consumidor). El procedimiento para calcular el troceo criptográfico que encripta y/o sella la clave 14C simétrica (o el procedimiento para usar tal troceo criptográfico para sellar la clave) es preferentemente un "secreto" conocido únicamente para herramientas de preparación de contenido confiables y aplicaciones de presentación confiables. Usar un troceo de esta manera puede complicar/desalentar la manipulación con los metadatos 12 contenidos con el libro electrónico 10. Se observa que puede usarse cualquier procedimiento para "sellar" un libro electrónico, siempre que tal procedimiento proporcione alguna medida de resistencia a manipulación para el libro electrónico 10.

De acuerdo con la presente invención, los metadatos 12 pueden incluir una etiqueta de derechos de autor, que describe los derechos concedidos al usuario o comprador mediante el origen de contenido (por ejemplo, el editor). Siempre que la etiqueta esté presente, el cliente (por ejemplo, el dispositivo 90 o 92 mostrado en la Figura 4) puede representar a un usuario el texto incluido en la etiqueta. Se apreciará que el acto de recordar a los usuarios las leyes de los derechos de autor que se aplican a sus libros electrónicos puede servir para disuadir que los usuarios típicos intenten copiar libros electrónicos.

Arquitectura de sistema de DRM

Como se muestra en la Figura 2, un sistema ejemplar para implementar la invención incluye un dispositivo de computación de fin general en forma de un ordenador personal o servidor 20 de red o similar, que incluye una unidad 21 de procesamiento, una memoria 22 de sistema, y un bus 23 de sistema que acopla diversos componentes de sistema incluyendo la memoria 22 de sistema a la unidad 21 de procesamiento. El bus 23 de sistema puede ser cualquiera de varios tipos de estructuras de bus incluyendo un bus de memoria o controlador de memoria, un bus de periféricos y un bus local usando cualquiera de una diversidad de arquitecturas de bus. La memoria de sistema incluye memoria 24 de solo lectura (ROM) y memoria 25 de acceso aleatorio (RAM). Un sistema 26 básico de entrada/salida (BIOS), que contiene las rutinas básicas que ayudan a transferir información entre elementos en el ordenador 20 personal, tal como durante el arranque, se almacena en la ROM 24. El ordenador personal o servidor 20 de red puede incluir adicionalmente una unidad 27 de disco duro para leer desde y escribir en un disco duro, no mostrado, una unidad 28 de disco magnético para leer desde o escribir en un disco 29 magnético extraíble, y una unidad 30 de disco óptico para leer o escribir en un disco 31 óptico extraíble tal como un CD-ROM u otro medio óptico. La unidad 27 de disco duro, la unidad 28 de disco magnético y la unidad 30 de disco óptico están conectadas al bus 23 de sistema mediante una interfaz 32 de unidad de disco duro, una interfaz 33 de unidad de disco magnético, y una interfaz 34 de unidad óptica, respectivamente. Las unidades y sus medios legibles por ordenador asociados proporcionan almacenamiento no volátil de instrucciones legibles por ordenador, estructuras de datos, módulos de programa y otros datos para el ordenador personal o servidor 20 de red. Aunque el entorno ejemplar descrito en el presente documento emplea un disco duro, un disco 29 magnético extraíble y un disco 31 óptico extraíble, debería apreciarse por el experto en la materia que otros tipos de medios legibles por ordenador que pueden almacenar datos que son accesibles por un ordenador, tales como cintas magnéticas, tarjetas de memoria flash, discos de vídeo digital, cartuchos Bernoulli, memorias de acceso aleatorio (RAM), memorias de solo lectura (ROM) y similares pueden usarse también en el entorno de operación ejemplar.

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

incluyen otros dispositivos de salida periféricos (no mostrados), tales como altavoces e impresoras.

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

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

Arquitectura de servidor

Haciendo referencia ahora a la Figura 3, se ilustra una primera arquitectura 70 de servidor ejemplar que implementa el sistema de DRM de la presente invención. La arquitectura 70 de servidor está implementada y desplegada en, por ejemplo, un sitio de venta minorista/distribución. En una realización de la invención, todos los componentes de la arquitectura 70 de servidor están asociados con una única parte (por ejemplo, una librería electrónica grande) que realiza tanto venta minoritaria de libros electrónicos 10 como realiza la descarga real de libros electrónicos 10 a los dispositivos de lectura de los clientes. En otra realización de la invención, los servidores 72 de librería y el objeto 74 COM de encriptación de URL están asociados con una parte (por ejemplo, un vendedor minorista de libros electrónicos 10 que no realiza descargas), y los otros componentes de la arquitectura 70 de servidor están asociados con una segunda parte (por ejemplo, un “alojamiento de ejecución”), que realiza descargas de libros electrónicos 10 que se comercializan/venden por la primera parte.

Las funciones proporcionadas mediante la arquitectura 70 de servidor incluyen: encriptación de libros electrónicos de origen, conversión al formato de lector de destino, generación de la construcción de licencia que define los derechos concedidos al usuario (en títulos de nivel 5), sellado del contenido antes de descarga de acuerdo con los requisitos (por ejemplo, un nivel de protección) expuestos por el proveedor de la publicación y descarga de títulos de libro electrónico. Esta arquitectura de servidor incluye también características que proporcionan una configuración flexible que posibilita a los usuarios de esta tecnología (proveedores de contenido, vendedores minoristas) escalar su sistema de acuerdo con sus necesidades. Estas características incluyen: resolución dinámica (a través de una consulta de base de datos) de ID de fichero a localizaciones de fichero físicas, almacenamiento en caché en memoria de las descargas más populares para eficacia superior y mejor rendimiento (donde la caché puede hacer expirar elementos basándose en, por ejemplo, una función de menos recientemente usado), y registro asíncrono de cada fichero descargado (también a una base de datos) para posterior auditoría/informe y/o fines de facturación. Pueden realizarse otras funciones mediante la arquitectura 70 de servidor de acuerdo con la presente invención.

Los servidores 72 de librería preferentemente son servidores Internet Information Server (IIS) de MICROSOFT® implementados en un servidor de red, tal como el ordenador 20 ilustrado en la Figura 2. Los servidores 72 de librería pueden comunicar con usuarios mediante software de exploración web (por ejemplo, proporcionando páginas web para ver con un explorador MICROSOFT INTERNET EXPLORER o un explorador NETSCAPE NAVIGATOR). A través de esta comunicación, los servidores 72 de librería pueden permitir que los usuarios hagan compras de títulos de libro electrónico, establezcan su relación de afiliación con el vendedor minorista, paguen por sus transacciones, y accedan a páginas de prueba de compra (recibos del lado de servidor). El objeto 74 de encriptación de URL puede residir en los servidores 72 de librería. El objeto 74 de encriptación de URL encripta un conjunto de parámetros relacionados con un libro electrónico que se ha comprado en el servidor 72 de librería. El objeto 74 de encriptación de URL puede encriptar estos parámetros usando un secreto (por ejemplo, una clave criptográfica simétrica) compartido entre el servidor 72 de librería y el servidor 76 de contenido web. Por ejemplo, los parámetros pueden incluir una identificación del libro electrónico comprado, información acerca de la compra tal como el nombre o número de tarjeta de crédito del comprador o un ID de transacción (por ejemplo, en el caso de títulos de nivel 3 o 5), y una indicación de tiempo. Se apreciará por los expertos en la materia que los parámetros anteriormente enumerados son ejemplares, y podrían usarse parámetros diferentes sin alejarse del alcance de la invención. Los parámetros encriptados pueden incluirse en una solicitud de HTTP que apunta al servidor 76 de contenido web, de manera que el servidor 76 de contenido pueda satisfacer la compra realizada en el servidor 72 de librería. Por ejemplo, después de que se ha seleccionado un libro electrónico por un comprador, el servidor 72 de librería podría cargar al dispositivo de computación del comprador una página web que contiene un enlace asociado con una solicitud POST, donde la solicitud POST apunta a un servidor de contenido tal como “www.content-provider.com”, y

el cuerpo del POST contiene los parámetros encriptados. En una realización alternativa de la invención, el enlace proporcionado en la página web podría asociarse con una solicitud GET, tal como "http://www.content-provider.com/isapi/ds.dll?action=download&value=<encrypted parameters>", aunque esta realización alternativa tiene la desventaja de que algunos exploradores pondrían un límite en el tamaño aceptable de un URL (por ejemplo, 2 kilobytes), restringiendo de esta manera el tamaño de los parámetros encriptados. Cualquiera que sea el tipo de la solicitud de HTTP está asociado con el enlace, el usuario podría a continuación seguir el enlace para iniciar la descarga. Puesto que los parámetros se han encriptado con un secreto compartido entre el servidor 72 de librería y el servidor 76 de contenido, es posible que el servidor 76 de contenido verifique que los parámetros encriptados se originaron en un servidor 72 de librería legítimo (por ejemplo, uno para el cual el operador del servidor 76 de contenido ha acordado proporcionar servicios de descarga). Si se incluye una indicación de tiempo, entonces el servidor 76 de contenido puede usar la indicación de tiempo para asegurar que los parámetros encriptados se generaron recientemente, resistiendo de esta manera a "ataques de reproducción" (es decir, "analizando paquetes" de la solicitud de HTTP por aquel que desea descargar libros electrónicos que él o ella no ha comprado legítimamente). El objeto 74 de encriptación de URL se implementa preferentemente como un objeto COM del lado del servidor, y se instancia preferentemente mediante Páginas de Servidor Activas (ASP).

Los servidores 76 de contenido son preferentemente servidores IIS implementados en un servidor de red (preferentemente diferente del servidor 72 de librería). Como el servidor 72 de librería, el servidor 76 de contenido puede implementarse en un ordenador tal como el ordenador 20 mostrado en la Figura 2. Se proporciona una extensión 78 de ISAPI de servidor de descarga, que es una DLL de extensión de IIS que preferentemente maneja las solicitudes entrantes a los servidores 76 de contenido. La DLL 78 de ISAPI es responsable de validar solicitudes de descarga, recuperar el fichero 10 de libro electrónico apropiado desde el almacenamiento 80 de contenido mediante el módulo 88 de extensión de almacenamiento de contenido, vender copias individualmente, devolver los títulos 10 de libro electrónico a los usuarios finales, y registrar la transacción en la base de datos 84 de ejecución mediante un módulo de mensajería asíncrona. El cliente 86 independiente de MICROSOFT Message Queue (MSMQ) es un módulo de mensajería asíncrona ejemplar que puede usarse en la arquitectura 70 de servidor (y la arquitectura 70' de servidor representada en la Figura 4 y analizada a continuación). Aunque se prefiere el uso de la tecnología de MSMQ de Microsoft para comunicación asíncrona de sus mensajes de servidor a servidor (cliente 86 de MSMQ), se apreciará por los expertos en la materia que puede usarse cualquier tecnología de mensajería de almacenar y reenviar. De acuerdo con un aspecto de la arquitectura 70 de servidor (y la arquitectura 70'), tal tecnología de mensajería resistente puede usarse para conseguir altos grados de fiabilidad y escalabilidad, puesto que toda la mensajería de servidor a servidor que no requiere comunicaciones en tiempo real se lleva a cabo usando una tubería de comunicaciones asíncrona.

El almacenamiento 80 de contenido es preferentemente un sistema de ficheros conectado en red grande o sistema de gestión de base de datos (o una pluralidad de tales sistemas de ficheros o sistemas de gestión de bases de datos). El almacenamiento 80 de contenido sirve como un repositorio para títulos LIT (libros electrónicos 10) usados mediante la ISAPI 78 de servidor de descarga cuando se satisfacen pedidos para los libros electrónicos 10. El almacenamiento 80 de contenido preferentemente expone una ruta de Convención de Nomenclatura Universal (UNC) que puede accederse mediante la ISAPI 78 de servidor de descarga. Por razones de seguridad, se prefiere que el almacenamiento o almacenamientos 80 de contenido existan detrás de un cortafuegos y no se expongan directamente a internet. La herramienta 82 de gestión y encriptación de contenido es un componente que realiza funciones tales como convertir contenido al formato LIT (por ejemplo, el libro electrónico 10), encriptar y sellar cada título de libro electrónico en el almacenamiento 80 de contenido. La herramienta 82 de gestión y encriptación de contenido también actualiza la base de datos 84 de ejecución con la localización física de cada fichero LIT en el almacenamiento 80 de contenido, que se mapea a su ID único en la base de datos 84 de ejecución. La herramienta 82 acepta ficheros de origen de texto sin cifrar (LIT, OEB, HTML, etc.) y genera ficheros LIT encriptados que están sellados de origen (por ejemplo, nivel 2), para recuperación posterior mediante la ISAPI 78 de servidor de descarga.

Haciendo referencia ahora a la Figura 4, se ilustra una segunda arquitectura 70' de servidor de acuerdo con la presente invención. La arquitectura 70' de servidor es un modelo distribuido, e incluye tres centros de datos: un sitio 71 de venta minorista, un sitio 73 de DRM y ejecución y un sitio 75 de activación. Como con la arquitectura 70 de servidor, la venta minorista de contenido y la ejecución de pedidos de contenido puede realizarse por una única parte, o una primera parte puede realizar venta minorista de libros electrónicos 10 mientras una segunda parte satisface pedidos para libros electrónicos 10 que se comercializaron por la primera parte. En este último escenario, el sitio 71 de venta está asociado con la primera parte y el sitio 73 de DRM y ejecución está asociado con la segunda parte. Dentro de la arquitectura de la Figura 4, se prefiere que todas las aplicaciones basadas en servidor web estén agrupadas detrás de una dirección de IP virtual, y que los servidores de contenido estén doblemente alojados. Se prefiere también que los servidores 94 de activación se basen en el sistema de afiliación PASSPORT™ de MICROSOFT® para asociar certificados a personas de usuario final, como se describirá a continuación (aunque PASSPORT es simplemente ejemplar de una autoridad de espacio de nombres que puede usarse para este fin).

Lo siguiente es una breve descripción de los componentes de la arquitectura 70' de servidor. Los servidores 72 de librería asociados con el sitio 71 de venta son servidores de red implementados en un ordenador tal como el ordenador 20. Preferentemente, los servidores 72 de librería ejecutan WINDOWS® 2000 Advanced Server que ejecuta IIS. Como en la arquitectura 70, estos servidores alojan el sitio web comercial que permite a los usuarios

realizar acciones tal como hacer compras de títulos de libro electrónico, establecer su relación de afiliación con el vendedor minorista, pagar sus transacciones y/o acceder a las páginas de prueba de compra (recibos del lado de servidor). El objeto 74 de encriptación de URL se proporciona para integración en el sitio 71 de vendedor minorista. Como en la arquitectura 70 de servidor, el objeto 74 de encriptación de URL de la arquitectura 70' de servidor puede implementarse como un objeto COM del lado de servidor instalado en los servidores 72 de librería e instanciarse mediante páginas de ASP, y puede encriptar parámetros relacionados con la compra de un libro electrónico 10 de manera que el servidor 76 de contenido puede validar los parámetros encriptados, autenticar al vendedor mediante un secreto compartido (por ejemplo, una clave simétrica usada para encriptar los parámetros), evitar ataques de reproducción y determinar el contenido para descargar a usuarios finales.

El servidor o servidores 76 de contenido/descarga son preferentemente WINDOWS® 2000 Advanced Server que ejecutan IIS. Los servidores 76 de contenido/descarga alojan los componentes principales de la aplicación de ejecución de DAS, incluyendo la extensión 78 de ISAPI de servidor de descarga, el módulo 88 de extensión de almacenamiento de contenido, el módulo 77 de servidor de licencia y el cliente 86 de tubería de ejecución.

Como se ha indicado anteriormente, la extensión 78 de ISAPI de servidor de descarga es preferentemente una DLL de extensión de IIS que maneja solicitudes entrantes a los servidores 76 de contenido. Es responsable de validar cada solicitud de descarga, sellar individualmente copias (cuando sea necesario), solicitar una licencia para copias completamente individualizadas (es decir, nivel 5) de libros electrónicos, devolver los títulos de libro electrónico a los usuarios finales, y registrar la transacción de descarga en una base de datos, tal como la base de datos 91 de registro.

El módulo 88 de extensión de almacenamiento de contenido es preferentemente una DLL que es responsable de determinar la localización física en el almacenamiento 88 de contenido de cada uno de los ficheros LIT (libros electrónicos) que se están descargando, basándose en una combinación de parámetros (por ejemplo, ID de libro y parámetros de tipo de ID de libro) incluidos en la solicitud de descarga (es decir, los parámetros encriptados anexados en el URL). El módulo 88 de extensión recupera también, desde la base de datos 89 de ejecución, información de configuración (por ejemplo, la clave privada del licenciatario y el certificado de clave pública, una lista de vendedores minoristas soportados y sus claves simétricas, etc.) requerida para inicializar la DLL 78 de extensión de ISAPI de servidor de descarga.

El módulo 77 de servidor de licencia es un subcomponente de la DLL 78 de extensión de ISAPI de servidor de descarga. Es responsable de generar y sellar licencias para ficheros LIT protegidos de nivel 5. Como se describirá más completamente a continuación, una licencia es una construcción que define los derechos que el usuario puede ejercer tras la compra de un título de libro electrónico. El módulo 77 de servidor de licencia 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 ejecución, que más tarde permite al lector 90 o 92 autenticar el canal de distribución cuando el fichero LIT descargado se accede en tal lector. Se describen completamente lectores ejemplares en el de Expediente del Mandatario N.º MSFT-0123, presentado concurrentemente con el presente, que se incorpora en el presente documento por referencia en su totalidad.

El cliente 86 de tubería de ejecución es preferentemente un cliente independiente de MICROSOFT® Message Queue (MSMQ), que está disponible con la familia de productos de WINDOWS® 2000 Server. Este componente implementa la tubería de comunicaciones asíncrona entre la ISAPI 78 de servidor de descarga y la base de datos 89 de ejecución. La ISAPI 78 registra cada transacción descargada mediante un mensaje publicado en el cliente 86 de MSMQ local en cada servidor 76 de contenido, que a su vez almacenará y reenviará tal mensaje en una forma resistente a un cliente 86 de MSMQ similar alojado en el servidor 84 de ejecución. Esta tubería se usará también para invalidar entradas almacenadas en caché en una caché de RAM de ISAPI (localizada en los servidores 76 de contenido), mediante mensajes que se publican desde el servidor 84 de ejecución a la DLL 78 de ISAPI mediante el mismo conjunto de clientes MSMQ alojados localmente.

Como en la arquitectura 70 de servidor, el almacenamiento 80 de contenido de la arquitectura 70' de servidor es preferentemente un sistema de ficheros conectado en red grande o sistema de gestión de base de datos. Sirve como un repositorio para los títulos LIT usados mediante la ISAPI 78 de servidor de descarga cuando se satisfacen los pedidos. Este servidor preferentemente ejecuta WINDOWS® 2000 Advanced Server y expone una ruta de UNC que puede accederse mediante la DLL de ISAPI de servidor de descarga. Esto puede conseguirse mediante una aplicación de configuración proporcionada mediante el DAS. Se prefiere también que el almacenamiento 80 de contenido exista detrás de un cortafuegos y no esté expuesto a la web.

El servidor 84 de ejecución es preferentemente un WINDOWS 2000 Advanced Server que ejecuta MICROSOFT® SQL 7.0 (o posterior). Este servidor aloja una base de datos 89 de ejecución, una base de datos 91 de registro, un cliente 86 de tubería de ejecución, y un objeto 87 COM de tubería de ejecución. La base de datos 84 de ejecución aloja tablas que mapean la combinación de un "ID de libro" y "tipo de ID de libro" a la localización física de cada fichero LIT en el almacenamiento 80 de contenido. La base de datos 84 también contiene información acerca de cada fichero LIT que puede requerirse para ejecución, tal como el título de libro, el autor del libro, el nivel de protección de DRM, y/o precio de venta minorista sugerido. El intervalo completo de información puede variar de acuerdo con las reglas/prácticas de negocio de cada centro de ejecución (por ejemplo, la entidad que opera el

servidor 76 de contenido), pero preferentemente la información incluye aquellos elementos anteriormente enumerados. Puede proporcionarse un guion de línea de comandos que crea las tablas necesarias y procedimientos almacenados para esta base de datos, además de añadir entradas de muestra que pueden usarse como referencia mediante el centro de ejecución cuando se diseñan sus procedimientos de gestión de contenido.

La base de datos 91 de registro se usa para registrar cada transacción de descarga desde la DLL 78 de ISAPI de servidor de descarga (para facturación/informe posterior cuando sea aplicable). El cliente 86 de tubería de ejecución es preferentemente un cliente independiente de MICROSOFT® Message Queue (MSMQ) que existe en los servidores 76 de contenido/descarga, como se ha descrito anteriormente. El objeto 87 de tubería de ejecución es preferentemente un objeto COM que se activa mediante el cliente independiente de MSMQ alojado en el servidor 84 de ejecución cada vez que se escribe un mensaje entrante en la cola de entrada en este servidor. El objeto 87 de tubería de ejecución extrae la información de registro desde cada mensaje MSMQ y la escribe a la base de datos 91 de registro, donde más tarde puede usarse por los guiones de informe. Adicionalmente, el objeto 87 de tubería de ejecución se activará mediante cambios en la base de datos 89 de ejecución e insertará cualquier información de actualización/borrado a los diversos clientes 86 independientes de MSMQ alojados en los servidores 76 de descarga.

La herramienta 82 de gestión de contenido es responsable de gestionar la información almacenada en la base de datos 89 de ejecución. Cuando se añaden ficheros LIT en el almacenamiento 80 de contenido, esta herramienta escribe los campos apropiados en la base de datos 89 de ejecución (por ejemplo, el ID de libro al mapeo de localización físico) de manera que el módulo 88 de extensión de almacenamiento de contenido pueda encontrar más tarde los ficheros LIT solicitados. De manera similar, si se hiciera cualquier cambio (por ejemplo, un cambio del nivel de DRM en un fichero LIT) esta herramienta proporciona la interfaz desde la cual los responsables de la función de gestión de contenido dentro del centro de ejecución (es decir, administradores de contenido humanos) llevarían a cabo estas tareas.

Los centros 73 de ejecución pueden completar la tarea de gestión de contenido creando un conjunto de páginas de ASP que, mediante objetos COM de IIS convencionales, escriben toda la información relevante en la base de datos 89 de ejecución y colocan el fichero LIT entrante (ya encriptado como una copia sellada de origen) en un servidor 83 de representación, que imitaría la estructura de directorio del almacenamiento 80 de contenido de producción. A partir de allí, los ficheros LIT se replicarían automáticamente usando, por ejemplo, el servidor de replicación de contenido Site Server 2000, en el servidor de almacenamiento de contenido de producción. El servidor 83 de representación no se requiere necesariamente para implementar el sistema DAS, pero es un enfoque ventajoso para replicar ficheros LIT desde la red del socio de ejecución en los servidores de almacenamiento de contenido de producción usando herramientas tales como el servidor de replicación de contenido (CRS) de MICROSOFT®.

Los servidores 94 de activación realizan la función de proporcionar a cada lector de cliente (por ejemplo, lector 90 de PC o dispositivo 92 de lectura especializado) con un repositorio seguro único y un certificado de activación. Un repositorio seguro ejemplar, y sistemas y procedimientos para proporcionar los mismos se desvelan en el de Expediente del Mandatario N.º MSFT-0126, presentado concurrentemente con el mismo, que se incorpora expresamente en el presente documento por referencia en su totalidad. El repositorio seguro y el certificado de activación asocian el lector activado con una persona en línea (por ejemplo, un ID de PASSPORT™ de MICROSOFT®) para asegurar que los usuarios podrán leer sus títulos adquiridos legítimamente en todos los casos de lectores que posean o que han activado para su persona (pero no en lectores no activados, o lectores no activados para esa persona) - suponiendo que activan sus lectores usando el mismo ID de usuario y contraseña cada vez.

El servidor 94 de activación incluye un objeto 96 PASSPORT y una DLL 98 de extensión de ISAPI de servidor de activación. El objeto 96 PASSPORT proporciona las interfaces requeridas en los servidores PASSPORT™ que autentican los usuarios finales usando, por ejemplo, sus cuentas de hotmail (y otros credenciales PASSPORT). De acuerdo con aspectos de la presente invención, este objeto asocia ventajosamente el certificado de activación con una persona, en lugar de un único PC, permitiendo por lo tanto a cada persona utilizar múltiples lectores para leer títulos de nivel 5. Aunque se apreciará que vincular títulos de nivel 5 a una “persona” permite uso más amplio de títulos de nivel 5 que si se unieran a un único dispositivo, definir una persona en términos de una autoridad de espacio de nombres establecida tal como los servidores PASSPORT sirve también el objetivo de limitar el uso no restringido de títulos de nivel 5 que pueden existir de otra manera si se permitiera a los usuarios usar una etiqueta arbitraria para funcionar como una persona. En el caso de credenciales PASSPORT, la información personal relacionada con un usuario particular está asociada con esos credenciales PASSPORT del usuario, posiblemente variando desde la cuenta de correo electrónico del usuario hasta su número de tarjeta de crédito. Por lo tanto, un usuario es improbable que comparta su ID de PASSPORT y contraseña con un gran grupo de personas, asegurando de esta manera que la persona para la que está activado un lector está asociada con un usuario particular (o, posiblemente, una familia que comparte una única cuenta PASSPORT). Aunque un servidor PASSPORT es una autoridad de espacio de nombres ejemplar que puede proporcionar esta característica ventajosa, se apreciará que podrían usarse otras autoridades de espacio de nombres sin alejarse del espíritu y alcance de la invención. En una realización alternativa de este tipo, el objeto 96 PASSPORT podría sustituirse con un objeto diferente que comunique con la autoridad de espacio de nombres alternativa.

La DLL 98 de extensión de ISAPI de servidor de activación lleva a cabo tareas asociadas con el procedimiento de activación en los servidores de activación de extremo frontal, incluyendo recibir un ID de hardware cargado mediante el cliente lector, crear un ID de máquina única basándose en la ID de hardware, publicar una solicitud en el servidor o servidores 100 de repositorio seguro, firmar cada repositorio seguro único recibido desde el servidor o servidores 100 de repositorio seguro, generar y (opcionalmente) encriptar el certificado de activación, actualizar la base de datos 102 de activación, y descargar tanto el repositorio seguro como el certificado de activación en el cliente lector. El procedimiento de activación se describe más particularmente a continuación en relación con la Figura 8.

Los servidores 100 de repositorio seguro son preferentemente servidores independientes localizados detrás de un cortafuegos en un centro de datos. Se acceden mediante los servidores 94 de activación para generar repositorios seguros individualizados para cada lector que está activado. Estos servidores son preferentemente especializados, y preferentemente ejecutan un servicio de WINDOWS® 2000 o WINDOWS NT® que expone una interfaz de conectores a los servidores 94 de activación. El servicio de repositorio seguro enlaza un ejecutable distinto para cada ID de máquina única y combinación de ID passport publicado. La tarea de preparar un repositorio seguro individualizado es, en muchos casos, computacionalmente intensiva. Por lo tanto, en una realización preferida existe un número suficiente de servidores 100 de repositorio seguros para proporcionar 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 102 de activación es preferentemente un servidor basado en MICROSOFT® SQL 7.0 que almacena información de activación relacionada con cada usuario final del lector 90 o 92 (basándose en sus ID de PASSPORT™). Tal información puede incluir: ID de máquina, el número de lectores activados, la fecha de primera activación, el ID de producto (PID) para cada una de las instalaciones de lector, su información de perfil PASSPORT™, etc. Esta información se usa para asegurar que los usuarios no están abusando del sistema, ayudar a los usuarios a recuperarse de fallos de disco duro y ayudar a permitir a los usuarios continuar leyendo el contenido que han comprado después de una mejora de hardware. Por ejemplo, el número de lectores activados y la fecha de la primera activación asociada con un credencial PASSPORT particular podría usarse para imponer un límite en el número de activaciones (por ejemplo, no más de cinco activaciones para una persona dada en los primeros 90 días después de la primera activación, con una activación adicional permitida cada 90 días posteriormente, 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 de lectores no comprobados activados para una única persona (que, en el peor caso, podría dar como resultado que un título de nivel 5 fuera legible en millones de dispositivos lectores, frustrando de esta manera el objetivo de controlar la distribución de contenido valioso). Adicionalmente, la otra información en la base de datos 102 de activación posibilita a los usuarios usar títulos de nivel 5 después de una mejora de hardware (o después de un fallo de disco duro), sin tener que volver a descargar títulos o licencias. En este caso, todo lo que un usuario necesita hacer es activar el lector en el hardware mejorado (o reparado) con el mismo ID de PASSPORT™.

El servidor 102 de base de datos de activación está localizado preferentemente detrás de un cortafuegos y únicamente es accesible mediante los servidores IIS de activación de extremo frontal en la misma red privada donde están localizados los servidores de repositorio seguro. Una réplica de la base de datos 102 de activación puede accederse mediante guiones fuera de línea para generar informes del número de activaciones por día, semana, mes, promedio de activaciones por ID de PASSPORT™, etc.

Infraestructura de recibo

Como se ha descrito brevemente antes, la arquitectura de servidor de la presente invención incluye un objeto 74 de encriptación de URL, que encripta ciertos parámetros relacionados con la venta de un libro electrónico 10, donde los parámetros encriptados son incluibles en un URL. Lo siguiente es una vista general más detallada del uso del objeto 74 de encriptación de URL.

El objeto 74 de encriptación de URL facilita un desacoplamiento del vendedor de libros electrónicos (por ejemplo, el vendedor minorista) de la entidad que realmente proporciona el fichero LIT al comprador (por ejemplo, un centro de ejecución). El objeto 74 de encriptación de URL realiza esta función encriptando información relacionada con el libro electrónico comprado con un secreto (por ejemplo, la clave 75 simétrica), que se comparte entre el centro de ejecución y el vendedor minorista. En un escenario ejemplar, el vendedor minorista entra en una relación empresarial (por ejemplo, un contrato) con un centro de ejecución, en el cual el centro de ejecución acuerda proporcionar servicios de descarga de contenido para el vendedor minorista que no tiene realmente un stock electrónico 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 vendedor y el centro de ejecución acuerdan en una clave 75 simétrica secreta, que se usará mediante el objeto 74 de encriptación de URL en el sitio del vendedor minorista, y mediante la DLL 78 de extensión de ISAPI en el sitio de centro de ejecución. Esencialmente, el vendedor minorista usa el objeto 74 de encriptación de URL y la clave 74 simétrica secreta para encriptar información relacionada con la compra de un libro electrónico, e incluye esta información encriptada como un parámetro a una URL que apunta al sitio de centro de ejecución. La URL se presenta a continuación en el software de exploración del comprador como una “página de recibo”, donde el “recibo” es un hiperenlace al URL que invoca la descarga desde el centro de ejecución. Cuando el usuario sigue el enlace, el centro de ejecución recibe el parámetro encriptado y lo desencripta usando la clave 75 simétrica secreta compartida. Puesto que el parámetro está

encriptado, cualquier información secreta que necesite intercambiarse entre el vendedor minorista y el sitio de ejecución puede proporcionarse de manera segura en forma encriptada al sitio del comprador, puesto que el comprador no conoce la clave 75 simétrica (y, presumiblemente, otros ojos escondidos en la web tampoco tienen acceso a la clave 75 simétrica). Además, cuando el centro de ejecución desencripta la información encriptada para obtener la información necesaria para la descarga, la desencriptación apropiada de la información autentica el "recibo" como que se ha generado mediante un vendedor minorista legítimo, puesto que presumiblemente ningún otro más que el vendedor minorista tiene la clave 75 simétrica necesaria para crear apropiadamente el parámetro encriptado. Debería observarse que la clave 75 simétrica es meramente ejemplar del tipo de secreto que podría compartirse entre un vendedor minorista y un centro de ejecución para permitir esta manera de comunicación. En una realización alternativa, podrían usarse pares de claves asimétricas, o el vendedor minorista y el centro de ejecución podrían acordar un procedimiento de encriptación sin clave secreta.

La Figura 5 representa el uso del objeto 74 de encriptación de URL para crear el parámetro encriptado. El objeto 74 de encriptación de URL encripta el parámetro de URL usando una clave 75 simétrica (el "secreto" de URL) que se comparte entre la ISAPI 78 de servidor de descarga y el objeto 74 de encriptación de URL en el servidor de venta minorista. En un escenario con alojamiento, donde un centro de ejecución proporciona la descarga de ficheros LIT comercializados por un gran número de sitios de venta minorista, se proporciona una clave 75 simétrica a cada vendedor minorista a medida que firman un contrato con el centro 73 de ejecución. Es importante observar que esta clave 75 simétrica puede ser única por vendedor minorista 71. El centro 73 de ejecución puede almacenar las claves para cada vendedor minorista en la base de datos 89 de ejecución. Debería observarse que la clave 75 simétrica usada para encriptación del parámetro de URL es diferente de las claves 14A simétricas generadas mediante la herramienta 82 de gestión y encriptación de contenido para encriptar los ficheros LIT.

Un único procedimiento exportado en el objeto 74 de encriptación de URL ("Encrypt()"), crea los parámetros de URL encriptados. Preferentemente el procedimiento Encrypt() toma los siguientes parámetros para incorporarse en el objeto binario grande encriptado que se usará en el URL:

ID de transacción (TransactionID) - una cadena que identifica de manera inequívoca cada transacción en el sitio 72 de librería;
ID de libro (BookID) - un identificador único, que se usa mediante el servidor 76 de descarga para localizar el fichero LIT apropiado mediante el módulo 88 de extensión de contenido (que consulta el ID de libro en la base de datos 84 de ejecución);
Tipo de ID de libro (BookIDType) - identifica de qué tipo es el ID (por ejemplo ISBN, DOI, PATH, etc.). El objeto 74 de encriptación de URL preferentemente no valida este campo, o su relación al ID. La ISAPI 78 de servidor de descarga posteriormente usar este campo como un parámetro de entrada adicional para la búsqueda realizada mediante el módulo 88 de extensión de almacenamiento de contenido;
Nombre de usuario (UserName) - una cadena que contiene el nombre del propietario legítimo del libro electrónico comprado. Esta cadena preferentemente mapea al consumidor listado en la tarjeta de crédito usada para la transacción comercial, aunque esto se deja como política para que se establezca mediante el origen de contenido (por ejemplo el editor) de acuerdo con el centro de ejecución. Esta cadena es el nombre que se usará más tarde mediante la ISAPI 78 de servidor de descarga para sellar individualmente los títulos (es decir para generar el exlibris). Se recordará que los títulos individualizados (por ejemplo, nivel 3 y nivel 5) incorporan el nombre de usuario en el fichero LIT y unen ese nombre a la clave de desencriptación, de modo que puede detectarse el origen de distribución no autorizada de contenido. Por lo tanto, se prefiere que el nombre del comprador provenga de una fuente fiable (tal como la tarjeta de crédito del usuario), en lugar de una fuente no verificable (tal como entrada de usuario). Aunque el ejemplo anterior supone que se insertará un nombre en este campo, los contenidos reales del capo se determinan mediante el vendedor minorista, y podrían contener cualquier información (por ejemplo, número de tarjeta de crédito, ID de transacción, ID de recibo, etc.) - preferentemente información que relaciona la compra o el comprador para permitir la vigilancia y rastreo de la copia;
ID de PASSPORT - el ID de la persona asociado con el usuario, que se proporciona mediante el usuario durante la activación. Este campo se usa posteriormente mediante el servidor de contenido para comparar con el ID de activación en el certificado de activación. Debería observarse que, aunque el ID de PASSPORT está contenido en el certificado de activación, ese ID no se carga al servidor 72 de librería durante la transacción de compra. En su lugar, el procedimiento de activación, además de insertar el ID de PASSPORT en el certificado de activación, almacena también el ID de PASSPORT en el registro en el dispositivo de computación del usuario, y es la instancia del registro del ID de PASSPORT que se proporciona al servidor 72 de librería; y
Nivel de seguridad (SecurityNivel) - esta cadena indica qué nivel de DRM requiere esta publicación particular. Esto se convertirá posteriormente en un número y se marcará en los metadatos 12 del título mediante la ISAPI 78 de servidor de descarga;
Opcionalmente, pueden incluirse también los siguientes parámetros de entrada con una solicitud:

Coste (Cost) - el precio que el comerciante (es decir, el vendedor minorista 71) pagó por ese título de libro electrónico en el momento en el que el título se vendió al consumidor;
MSRP - precio recomendado del editor en el momento que se vendió el título;
Precio (Price) - el precio por el que se vendió el título de libro electrónico. Esto es un parámetro opcional, y si está presente se usará mediante el servidor de descarga para fines de registro y, potencialmente, para fines

de facturación;
Nombre de Fichero Amigable (FriendlyFileName) - esta cadena se usa mediante el servidor de descarga cuando se establece el nombre de fichero para el fichero LIT que se está descargando mediante el encabezamiento de HTTP de respuesta; y
ID de cliente (CustomerID) - un identificador único para usuario final que compra el título de libro electrónico. El comerciante (es decir, el vendedor minorista 71) puede requerir esta información como parte de los informes que recibe desde el centro de ejecución.

La lista de parámetros anterior es extensible y no debería interpretarse como que limita el conjunto completo soportado mediante el objeto 74 de encriptación de URL. Pueden añadirse pares de atributo-valor adicionales, puesto que el objeto 74 de encriptación de URL encriptará el conjunto total de valores pasados y los devolverá a la función de llamada.

Preferentemente, el objeto 74 de encriptación de URL añade una indicación de tiempo y versión. La indicación de tiempo es la cadena que preferentemente contiene una representación del número de nanosegundos pasados desde 1601 (en tiempo de sistema GMT) en la máquina local donde está instalado el objeto 74 de encriptación de URL. Este valor puede usarse mediante el servidor de descarga para calcular un tiempo de vida (TTL) para evitar ataques de reproducción (es decir, alguien que robe un URL y lo reproduzca para descargar un libro. El campo de versión es una cadena desencriptada que identifica la versión del objeto 74 de encriptación de URL que creó el objeto binario grande encriptado en el URL.

Después de que el vendedor minorista 71 obtiene la cadena encriptada de vuelta del objeto 74 de encriptación de URL, el vendedor minorista 71 crea una solicitud de POST que apunta al servidor 76 de descarga para ejecución. El objeto binario grande encriptado devuelto mediante el objeto 74 de encriptación de URL está incluido en el cuerpo de cada POST. Además de los parámetros encriptados, los vendedores minoristas pueden necesitar proporcionar un ID de vendedor minorista (RetailerID) en el URL que identifica al vendedor minorista. Este puede usarse mediante la DLL 78 de ISAPI de servidor de descarga para mapear la solicitud de entrada a la clave 75 simétrica de URL apropiado para desencriptación en caso de que se soporten múltiples vendedores por un único sitio 76 de servidor de descarga. Este es un campo opcional y si no se proporciona, la DLL 78 de ISAPI de servidor de descarga en el sitio 73 de ejecución usará más tarde su clave 75 simétrica por defecto proporcionada durante la configuración para desencriptar los URL.

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

TransactionId=R6RAKHAL9TS12JTG00QP9ESTQ4&BookId=044021145X&BookIdT

ype=ISBN&Username=Pavel+Zeman&SecurityLevel=3

El objeto 74 COM de encriptación puede devolver el siguiente objeto binario grande encriptado:
LCfsQCLuMg9UZtWxIdYTfw%2BzMtjXAN%2BiU0YHaomrY3ydXhw3p9TlwZuH%
2BFEHTEP687Nq17wbMMwnbtHAkIjkKhKS%2BYKwgHj7%2FNr%2BvBD50APwq
MbvN3saNBrPxG8s1ziU1iX%2F%2BSS%2FttA%2F4GZjRMo5uXWM%2BZr5dYHk
SfWfBBC0iH7uLFolyIz8LSI=&Version=1.0

El URL del objeto 74 de encriptación de URL codifica el objeto binario grande encriptado, de manera que cumple con la norma de HTTP requerida para los URL de ANSI. El objeto 74 de encriptación de URL acepta tanto cadenas Unicode como UTF-8, y maneja conversión UTF-8 desde Unicode internamente. Opcionalmente, el objeto 74 de encriptación de URL usa UTF-8, si se proporciona, que reduce el tamaño del objeto binario grande escapado final encriptado resultante para entrada no Unicode en aproximadamente una mitad. El objeto 74 de encriptación de URL preferentemente calcula un troceo criptográfico de los datos a encriptar antes de encriptar tales datos, e incluye el troceo con (por ejemplo, delante de) los datos encriptados y codificados. Este troceo puede usarse posteriormente para comparación mediante el servidor de descarga para verificar que los datos desencriptados no se han manipulado entre el sitio de venta minorista y el servidor de descarga. Por ejemplo, el parámetro completo (por ejemplo, a incluirse en el cuerpo de una solicitud de POST), puede leerse:

VALUE="&Hash=bCt/xn4lfTJw7cPQjstge+6Lifc=&Data=zAybPKW123

d2O+... datos_codificados_continuan ...MSSD8Eyw==&Version=1.5"

La ISAPI 78 de servidor de descarga es responsable de la individualización y descarga de títulos de libro electrónico a usuarios finales. También, el análisis y validación de cada URL generado mediante el objeto 74 de encriptación de URL se realiza mediante la DLL 78 de ISAPI de servidor de descarga. Esto incluye desencriptar el URL usando la clave 75 simétrica apropiada, que puede ser una clave por defeco o, en el caso donde se proporcione un ID de vendedor minorista, una cadena resultante de una consulta de base de datos mediante el módulo de extensión de almacenamiento de contenido. La DLL 78 de ISAPI de servidor de descarga resuelve también el mapeo de ID de libro y tipo de ID de libro desde el URL pasado en una localización de compartición de ficheros preferentemente mediante un módulo de extensión. El módulo de extensión recupera esa información desde la base de datos de

ejecución y posibilita a los proveedores de contenido añadir su propia base de datos de mapeo y reglas de convención de nomenclatura.

La ISAPI 78 de servidor de descarga también determina el nivel de protección de DRM requerido para la descarga del fichero LIT solicitado. El nivel se determinará basándose en una indicación desde la base de datos 89 de ejecución del nivel de DRM para el título que se está descargando. Por ejemplo, si el URL creado por el vendedor minorista define un nivel de DRM inferior que el especificado en la base de datos de ejecución, se devolverá un mensaje de error al vendedor minorista 71. También, la ISAPI capturará el título de libro electrónico para descargar desde el almacenamiento 80 de contenido en una caché de memoria local, si no está almacenado en la caché, quita la clave 14A simétrica (véase la Figura 1) desde el fichero LIT antes de almacenarla en caché localmente en el servidor IIS, y almacena en caché la clave 14A en memoria para uso futuro.

En el caso de títulos de DRM de nivel 3, la ISAPI 78 de servidor de descarga inserta el nombre del usuario desde el objeto binario grande de URL encriptado en el fichero LIT como un flujo separado, vuelve a trocear los metadatos con los contenidos de este nuevo flujo, sella la clave 14A simétrica con el troceo criptográfico recién calculado, y vuelve a insertar la clave simétrica recién sellada en el fichero LIT para descarga. En el caso de títulos de DRM de nivel 5, la ISAPI de servidor de descarga genera una estructura de XML de licencia (además de las acciones de nivel 3 anteriormente indicadas), sella la clave simétrica con la clave pública desde el certificado de activación del usuario final, y embebe la licencia en el fichero LIT.

La ISAPI 78 de servidor de descarga también descarga el fichero LIT al usuario final, libera el almacenamiento temporal usado durante la individualización del fichero LIT, y registra cada solicitud de descarga en cualquiera de un fichero local en el servidor IIS o en la base de datos 91 de registro, mediante la tubería de ejecución asíncrona analizada a continuación. Esto puede realizarse mediante una publicación de mensaje en el cliente MSMQ local residente en cada servidor 76 de descarga.

La DLL 78 de extensión de ISAPI de servidor de descarga responde a un conjunto de comandos definidos mediante el parámetro “?action=“. Preferentemente, hay dos acciones soportadas mediante la ISAPI 78 de servidor de descarga: descargar y verificar. La acción de descarga es el comando que provoca que la ISAPI 78 siga las etapas identificadas en la Figura 7 y devuelva un título de libro electrónico al usuario. La acción de verificación se usa para solicitar que la ISAPI 78 verifique que existe un ID de libro dado en el almacenamiento 80 de contenido y está listo para descargar. El comando más común (descarga) puede parecer como el siguiente URL:

http://content-provider.com/isapi/ds.dll?action=download&value=...

El parámetro /isapi/ en el URL indica la raíz virtual donde estaba instalada la ISAPI 78. En este ejemplo la ISAPI 78 se denomina ds.dll (DLL de servidor de descarga). El nombre de ISAPI 78 se sigue por la acción, que se sigue por los parámetros relevantes para llevar a cabo esa acción (el parámetro “valor” en el ejemplo anterior). En estos ejemplos, los parámetros relevantes comprenden el objeto binario grande encriptado generado mediante el objeto 74 COM de encriptación de URL.

Cada solicitud de descarga incluirá, en el cuerpo del POST, el URL para la página de manejo de errores en el sitio 71 del vendedor minorista. El servidor 76 de descarga usa este URL cada vez que tiene lugar un error y redirige al cliente a esa página, con el código de error etiquetado en la cadena de petición. En el caso de un error, los vendedores pueden proporcionar una UI de HTML, un número de soporte, un enlace de correo electrónico o instrucciones de resolución de problemas. De acuerdo con un aspecto de la presente invención, la DLL 78 de ISAPI de servidor de descarga preferentemente no presenta errores, sino en su lugar, redirige a los usuarios al URL de manejo de errores requerido desde la solicitud POST.

Desde los puntos de vista de gestión y operabilidad de un centro de datos, la ISAPI 78 expondrá contadores de rendimiento (es decir, contadores PerfMon) y eventos de WINDOWS NT®. Estos son prácticas operacionales de WINDOWS® 2000 y WINDOWS NT® típicas para despliegue y gestión de centro de datos de componentes de servidor. Los eventos de WINDOWS® 2000 y WINDOWS NT® se registran cada vez que tiene lugar un error. Alguno de los eventos clave que se registran preferentemente por la ISAPI 78 son:

Fallo al inicializar - cualquier configuración perdida y/o ajuste de entorno requerido que produjo que fallara la ISAPI en carga;

Fallo al conectar al almacenamiento de contenido - cualquiera de la ruta UNC devuelta mediante el módulo de extensión de almacenamiento de contenido que fuera inválida o el almacenamiento 80 de contenido y/o ruta de red hasta él esté caída. En cualquier caso, la ISAPI debe registrar un error de manera que los operadores del centro de datos puedan tomar la acción apropiada;

Solicitud de URL ilegal - este evento debe registrarse cada vez que una solicitud de URL no cumpla con el formato esperado o no se haya encriptado mediante la clave 75 simétrica compartida entre la ISAPI 78 y el objeto 74 COM de URL. Idealmente, el URL completo debería publicarse en el evento, junto con la IP de origen, para fines de auditoría;

Fallo al localizar un fichero LIT - la ruta en la solicitud fue inválida o el fichero LIT está perdido desde la compartición de destino;

Fallo al almacenar en caché el fichero LIT - esto puede ocurrir si el servidor 76 de contenido que aloja la ISAPI 78 se queda sin memoria, o si tuvo lugar un problema de red durante la transmisión de fichero desde el almacenamiento 80 de contenido;
Fallo al crear el exlibris - este evento debe registrarse cada vez que la ISAPI 78 no puede llevar a cabo el sellado individual del título. La naturaleza del error debe incluirse en el propio evento, para depuración posterior;
Fallo al descargar el título - este evento debe registrarse siempre que falla una descarga (tiempo agotado, o conexión interrumpida, etc.); y
Eventos de arranque/cierre - siempre que la ISAPI 78 se (des)carga, debe registrar un evento de información para este punto, de manera que exista visibilidad apropiada. Puede haber casos cuando una ISAPI 78 se descarga mediante el IIS y los operadores de centro de datos necesitan volver a iniciar el IIS o incluso WINDOWS NT® para acceder al servidor 76 de contenido de vuelta a un estado completamente operacional.

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

Solicitudes de descarga totales - medidas en solicitudes únicas aceptadas desde el último arranque del servidor;
Descargas satisfactorias totales - medidas en solicitudes únicas cumplimentadas desde el último arranque del servidor;
Solicitudes de descarga/s - número de solicitudes entrantes únicas/s;
Descargas satisfactorias/s - medidas en solicitudes únicas cumplimentadas por segundo;
Solicitudes de descarga pendientes - número total de solicitudes que se han procesado en cualquier momento dado;
Solicitudes de descarga fallidas - número total de fallos desde último arranque del servidor;
Tiempo de procesamiento de solicitud medio - medido en milisegundos, refleja el tiempo medio que la ISAPI está tardando en procesar solicitudes entrantes; y
Tiempo de procesamiento de última solicitud - medido en milisegundos, refleja el tiempo que tardó para la ISAPI procesar su solicitud más reciente;
Combinados, los eventos de WINDOWS NT® y los contadores PerfMon permitirán a un anfitrión de conjuntos de monitorización y gestión de centro de datos existentes administrar la ISAPI 78 durante el despliegue del sistema.

Tubería de ejecución asíncrona

La tubería de ejecución asíncrona realiza registro asíncrono de solicitudes de descarga en la base de datos 91 de registro e invalidaciones asíncronas de entradas almacenadas en caché mediante la DLL de ISAPI de los servidores de descarga. El servidor de tubería de ejecución asíncrono consigue estas tareas aprovechando la funcionalidad de almacenar y reenviar existente proporcionada mediante el componente MICROSOFT® Message Queue (MSMQ) de Windows® 2000.

La arquitectura para la tubería de ejecución se muestra en las Figuras 4 y 6. El objeto 87 de tubería de ejecución se ejecuta mediante el servicio de activación de MSMQ y escribe en la base de datos de registro cada vez que aparece un mensaje entrante en la cola de entrada del cliente 86 de MSMQ local. Preferentemente, el objeto 87 de tubería de ejecución se implementa como un objeto COM. El agente 85 de actualización de caché tiene un ejecutable asociado que se genera mediante un activador de SQL cada vez que tiene lugar una actualización u operación de borrado en la base de datos 89 de ejecución. La DLL 78 de extensión de ISAPI de servidor de descarga tanto leerá como escribirá a/desde el cliente 86 independiente de MSMQ local.

Una función de registro se ejecuta preferentemente en la base de datos 91 de registro para hacer persistir todos los parámetros que se pasan en el cuerpo de cada solicitud POST para descargas. El objeto 87 COM de tubería de ejecución se instancia en el servidor 84 de ejecución a medida que llega cada mensaje de registro individual en la cola de entrada del cliente 86 independiente de MSMQ local en el servidor 84 de ejecución. El esquema de la base de datos 91 de registro se describe en mayor detalle a continuación. La información desde el cuerpo de cada solicitud de POST a los servidores 76 de descarga se convierte en un formato de mensaje de MSMQ y se publica en la cola de entrada del cliente 86 de MSMQ local en el servidor 84 de ejecución.

El cliente 86 de MSMQ en el servidor 76 de ejecución a continuación coge este paquete de mensaje e invoca, mediante el servicio de activadores de MSMQ, el objeto 87 COM de tubería de ejecución, que convierte el mensaje a formato de base de datos y lo escribe en la base de datos, mediante un Nombre de Origen de Datos (DSN) en el servidor 84 de ejecución que resume el nombre, localización y credenciales de registro para la base de datos de registro desde el objeto COM.

A medida que la herramienta 82 de gestión de contenido actualiza y/o borra registros desde la base de datos 89 de ejecución, se activa un ejecutable 85 de agente de actualización de caché mediante el servidor de SQL (usando activadores de actualización/borrado de SQL convencionales). El agente 85 de actualización de caché realiza una función similar al objeto 87 COM de tubería de ejecución, pero en la dirección opuesta. Dado que las operaciones de actualización y borrado en la base de datos 89 de ejecución pueden requerir actualizaciones de caché en las DLL 78 de ISAPI de servidor de descarga de extremo frontal, este agente formará un mensaje de MSMQ y lo publicará a través del cliente 86 de MSMQ independiente a todos los servidores 76 de descarga (el servidor 84 de ejecución debería tener una lista de todos los servidores 76 de descarga instalados).

Al recibir el mensaje de actualización de caché, el cliente 86 de MSMQ en el servidor 76 de descarga llama una función en la DLL 78 de extensión ISAPI para actualizar la caché. Esta acción elimina la entrada de caché. La siguiente vez que se recibe una solicitud para este ID de libro particular, el servidor 76 de descarga pedirá de nuevo a la base de datos 84 de ejecución y a continuación actualiza la caché con el nuevo fichero LIT y sus atributos relevantes. El tamaño de la caché para el servidor 76 de descarga se determina mediante la cantidad de memoria libre en el servidor físico. Se prefiere que la DLL 78 de ISAPI asigne hasta el 80 % de la memoria disponible en el servidor.

Generación de licencia

Las licencias se generan preferentemente para todos los títulos firmados y completamente individualizados (es decir, nivel 5). La publicación de origen puede acompañarse también mediante una licencia que constituye la firma de origen, asegurando por lo tanto la autenticidad del libro electrónico que se ha comprado por el consumidor. Las licencias pueden delegarse y la cadena de licencia preferentemente se origina en los proveedores de publicación (es decir, autores y editores) y finaliza en el consumidor que compra. De acuerdo con la presente invención, los derechos preferentemente pueden delegarse por los licenciatarios pero no por los consumidores. Una licencia de usuario final se genera típicamente en el momento de descarga. En algunos casos, el vendedor minorista nombrará el propietario legítimo del libro electrónico (en el caso de sellar individualmente) en la licencia, que se expone posteriormente mediante la UI (mediante una característica del lector 90 o 92) cuando los consumidores abren sus libros electrónicos.

Haciendo referencia ahora a las Figuras 4 y 7, 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 incorporada en el objeto binario grande de URL encriptado) se analiza para atributos (etapa 112). Si la solicitud se forma bien en la etapa 114, a continuación se determina si la solicitud es para una licencia de nivel 5 (etapa 118). Si no, a continuación en la etapa 116, se devuelve un error y el procedimiento se detiene.

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 principios del usuario. Si se proporcionaron, entonces los principios se hacen persistentes en una base de datos local en la etapa 130. Si no, entonces en la etapa 122, se determina si los principios de usuario pueden recuperarse desde una base de datos local. Si no, se capturan desde el servidor de registro en la etapa 124, y si son satisfactorios (etapa 126), los datos se hacen persistir en la base de datos local en la etapa 130. Si la solicitud para capturar los datos desde el servidor de registro falló en la etapa 126, a continuación se registra un evento (etapa 128) y el procedimiento finaliza en la etapa 146.

Si en la etapa 122, los principios de usuario pueden recuperarse desde la base de datos local, a continuación el procesamiento continúa en la etapa 132, donde se encripta la clave simétrica con la clave pública del usuario desde el certificado. La etapa 132 se realiza también después de que se hacen persistir los principios del usuario en la base de datos local en la etapa 130. El procesamiento a continuación continúa a la etapa 134, donde se determina si la licencia es individualizada. La etapa 134 es también cuando 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 es individualizada, se incluye el nombre del usuario en la licencia como el propietario legítimo. El procesamiento continúa en la etapa 136 donde se completa la estructura de XML de la licencia con el nombre del usuario y se firma. Si en la etapa 134, la licencia no es individualizada, el procedimiento a continuación continúa en la etapa 138 donde se completa la estructura de XML de la licencia (sin el nombre del usuario) y se firma. En la etapa 140 se determina si la generación de licencia tuvo éxito. Si es así, a continuación se actualizan los contadores de rendimiento y se devuelve el fichero de XML de la licencia (etapa 144), y, si no, se registra un evento y se devuelve un error (etapa 142). El procesamiento a continuación se completa en la etapa 146.

Una vez que se ha iniciado una descarga en el centro 73 de ejecución (es decir, los usuarios han realizado un pedido y a continuación han hecho clic en el enlace para descargar), en el caso de un título completamente individualizado la DLL 78 de ISAPI de servidor de descarga preferentemente publica una solicitud al módulo 77 de licencia para generar una licencia única para el título de libro electrónico que se está descargando. El URL de solicitud de descarga debe proporcionar, como parte de los parámetros encriptados, información de manera que el módulo de licencia pueda sellar individualmente cada licencia. Estos parámetros incluyen, para copias de nivel 5, el certificado de activación encriptado descargado al usuario final durante la activación de su software de lector. Un libro electrónico con licencia no puede abrirse a menos que la licencia requerida esté presente y disponible para el lector.

Después de que los usuarios compran sus dispositivos de libro electrónico o descargan el software 90, 92 de lector de internet, estarán alentados a activar sus lectores la primera vez que se lancen (por ejemplo, inmediatamente después de la configuración de la aplicación de lector de portátil/sobremesa). La activación posibilita al software de lector a la compra de copias protegidas de nivel 5 completamente individualizadas. El flujo de procedimiento de la activación de lector, la experiencia de usuario final y las interacciones de cliente-servidor que tienen lugar se describirán ahora.

Cada vez que se lanza el lector 90 o 92, comprueba para ver si se ha activado. Si no, el lector presentará un cuadro de diálogo recordando al usuario que no podrá obtener títulos especiales que requieren individualización completa para distribución a menos que el usuario active el lector. Los usuarios pueden activar el lector desde cualquier sitio web de venta minorista, mientras hacen compras con un explorador independiente, o desde una característica de "librería integrada" del lector (que permite la comunicación con sitios de librería usando el propio software de lector en lugar de software de exploración de fin general). Aún además, el lector puede activarse desde dentro de un sitio del comerciante, mientras hace compras dentro de la característica de librería integrada del lector. Este escenario de activación puede tener lugar si, por ejemplo, el usuario declinó activar el lector durante el primer lanzamiento y ahora desea comprar un título completamente individualizado (nivel 5 protegido), que requiere activación.

Suponiendo que el usuario ha aceptado activar el lector como se ha mencionado anteriormente, el procedimiento que sigue incluirá las siguientes etapas, como se ilustran con respecto a las Figuras 4 y 8.

En la etapa 150, el cliente lector abre la característica de biblioteca integrada y conecta, mediante la capa de conexión segura (SSL), a los servidores 94 de activación, donde se solicita a los usuarios iniciar sesión usando, en este ejemplo, sus credenciales PASSPORT™ (etapa 152). Si el usuario no tiene una cuenta PASSPORT™, él/ella se le proporcionará con un enlace para inscribirse para una (etapa 154). Se prefiere que el URL al servidor 94 de activación esté pregrabado permanentemente en un control de ActiveX de Activación usando una conexión de SSL de manera que el cliente pueda garantizar que los servidores son verdaderamente los servidores 94 de activación.

Una vez que se han autenticado los credenciales PASSPORT™ del usuario (etapa 156), se hace una petición a una API de PASSPORT™ para el alias del usuario y dirección de correo electrónico (etapa 158). Posteriormente, en las etapas 160-162, los servidores 94 de activación solicitarán que el cliente (mediante el control de ActiveX) carguen un ID de hardware único (por ejemplo, que, como se ha indicado anteriormente, pueda deducirse desde componentes de hardware en el dispositivo de computación del usuario que sustancialmente identifican de manera inequívoca el dispositivo de computación del usuario). A continuación, se determina en la etapa 164 si esta es una nueva activación para el lector (a diferencia de una "recuperación" de una activación anterior).

Si se determina que es una nueva activación en la etapa 164, a continuación el procedimiento continúa a la etapa 168 para determinar si se ha alcanzado un límite de activación. Si se ha alcanzado el límite, a continuación se presenta un mensaje de error en la etapa 172, que incluye preferentemente un número de teléfono de soporte. El procedimiento a continuación finaliza en la etapa 198. De acuerdo con una característica de la presente invención, puede limitarse a los usuarios en cuanto al número de activaciones que pueden realizar, y/o la frecuencia a la que pueden realizarlas (es decir, cuántos lectores diferentes pueden activar para leer títulos de nivel 5 comprados bajo una persona dada). En el ejemplo de la Figura 8, se limita a los usuarios a cinco activaciones en 90 días después de la primera activación del lector. Esto permite a los usuarios activar sus propios lectores, mientras se evitan abusos del sistema de DAS. Un ejemplo del tipo de abuso que evita un límite de este tipo sería un club de lectores que comprara un libro electrónico con su cuenta PASSPORT y permitiera a miles de sus miembros activar sus lectores con los credenciales PASSPORT del club de lectura. El límite sobre las activaciones puede permitir también activaciones adicionales a medida que pasa el tiempo - por ejemplo, una activación adicional por cada periodo de 90 días después de los primeros 90 días, hasta un límite de 10 activaciones totales. Se apreciará que estos límites son meramente ejemplares, y puede usarse cualquier límite en las activaciones sin alejarse del espíritu y alcance de la invención.

Si el usuario no ha activado los cinco lectores en los primeros 90 días (o ha alcanzado un límite de activación aplicable diferente), se presenta una página de activación en el dispositivo del usuario (etapa 170). Cuando el usuario vuelve al formulario, los servidores de activación determinan si el formulario está completo (etapa 174); si el formulario no está completo, el procedimiento vuelve a la etapa 170 para volver a presentar el formulario hasta que el usuario complete el formulario. A continuación en la etapa 176, se determina si esta activación es una recuperación. Si no es una recuperación, entonces se crea un nuevo registro para el usuario y lector y el número de lectores activados para ese usuario se incrementa (etapa 180). Un par de claves de repositorio seguras pre-generadas se recuperan desde una base de datos (etapa 182) y se generan también certificados de activación (etapa 184). Las claves de activación, ID de usuario e ID de máquina se hacen persistir en una base de datos en la etapa 186. En un ejemplo, cada usuario (es decir, persona, según se identifica mediante, por ejemplo, la cuenta PASSPORT) se asigna un par de claves de activación que se usan en el certificado de activación para cada lector que el usuario activa, caso en el que la clave 14A simétrica de los títulos de nivel 5 está encriptada con la clave pública en el par de claves de activación en el momento en que se prepara el título para ese usuario mediante el sitio 73 de ejecución. En un refinamiento adicional de ese ejemplo, cada dispositivo de lectura está equipado con un repositorio seguro único individualizado que tiene un par de claves único asociado con él, donde el certificado de activación para un dispositivo dado contiene su clave privada en un formulario encriptado mediante la clave pública asociada con el repositorio seguro. De esta manera, para presentar un título de nivel 5 es necesario que estén presentes tanto el repositorio seguro como el certificado de activación, puesto que el repositorio seguro usa su clave privada para desencriptar la clave privada del certificado de activación, que, a su vez, se usa a continuación para desencriptar la clave 14A simétrica del título de libro electrónico, que, a su vez, se usa para desencriptar el flujo 16 de contenido 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, a continuación (en la etapa 178) se generan 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 repositorio seguro individualizado ejecutable (vinculado al ID de la máquina descargado) y un certificado de activación (vinculado al ID del PASSPORT™ del usuario). El repositorio seguro ejecutable y el certificado de activación se descaran a continuación al cliente (etapas 188 y 190). El certificado de activación se encripta (por razones de privacidad) y se carga más tarde mediante el cliente al servidor de descarga para preparar copias completamente individualizadas (títulos protegidos de nivel 5). El ID del PASSPORT™ del usuario puede encriptarse y marcarse en el registro del PC como parte de esta descarga, para carga durante transacciones comerciales. Este procedimiento puede asegurar que el ID de PASSPORT™ incluido en el URL para descargar coincide con el del certificado de activación que está incluido en el cuerpo del Post, para evitar robo de contenido.

En la etapa 192 se determina si la descarga fue satisfactoria. Si no, se registra un evento y se intenta de nuevo la descarga (etapas 194 y 192). Si la descarga fue satisfactoria, a continuación en la etapa 196, se proporciona al usuario con una “página de felicitación” y se informa que la activación está completa. La “página de felicitación” puede proporcionar también un enlace para canjear libros gratis promocionales en este momento, como una manera para alentar a los usuarios a activar sus lectores. Este enlace puede aprovechar un procedimiento expuesto mediante el control de ActiveX de activación para devolver al usuario a una página de biblioteca en el lector. El procedimiento a continuación finaliza en la etapa 198.

Se prefiere que una vez que el lector se conecta a los servidores 94 de activación, que los servidores 94 controlen toda la experiencia del usuario mediante páginas ASP y HTML. Estas páginas se ajustan preferentemente a especificación convencional, y usarán los procedimientos de guía de estilo y java script proporcionados para asegurar una experiencia sin interrupciones que es consistente con la “apariencia y sensación” de la interfaz de usuario del lector.

Parte del procedimiento de activación para el lector de plataforma abierta (por ejemplo, una aplicación de software de lector instalada en un PC) es la individualización de repositorio seguro y posterior descarga. Como se analiza en mayor detalle en el de Expediente del Mandatario N.º MSFT-0126, presentado concurrentemente con el presente e incorporado en el presente documento por referencia en su totalidad, se proporciona un componente de servidor (por ejemplo, el servidor 100 de repositorio seguro, mostrado en la Figura 4) que es responsable de individualizar módulos de software de repositorio seguros para cada instancia del lector para plataformas abiertas (por ejemplo, ordenadores de portátil y sobremesa). El repositorio seguro único oculta las claves criptográficas usadas en el procedimiento para desellar y desencriptar los ficheros LIT de nivel 5, así como asegurar que el contenido de nivel 5 desencriptado no se escapa del sistema controlado, y, puesto que es individualizado para una instalación de hardware particular, resiste la portabilidad y, si se rompiera, su individualización resiste usando las mismas técnicas de ruptura en un repositorio seguro diferente instalado en hardware diferente.

Como se ha indicado anteriormente, un aspecto para resistir el abuso del sistema de DRM es limitar el número de activaciones que cualquier usuario particular pueda tener con un único ID de PASSPORT™. Si este número no está limitado, los usuarios deshonestos pueden inscribirse en un PASSPORT™ de “dominio público”, compartir a continuación los credenciales para esa cuenta con todos sus amigos (o peor, publicarlo en la Web), junto con todos los libros electrónicos que hayan comprado. Esto creará rápidamente una cadena de piratería, puesto que cualquier usuario que activara el lector con los credenciales de PASSPORT de “domino público” podría a continuación leer 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 “cuotas” de activación que permitan a los usuarios activar lectores en múltiples dispositivos que poseen (por ejemplo, un portátil, sobremesa, PC de bolsillo, libro electrónico, etc.) así como permitirles activar nuevos dispositivos a medida que mejoran su hardware, reformatean sus discos duros, etc., sin permitir activaciones no comprobadas e ilimitadas de lectores para los mismos credenciales de PASSPORT. La experiencia pasada con el comportamiento del usuario sugiere que los usuarios legítimos activan un lector (o un número pequeño de lectores) inicialmente, y a continuación pueden activar nuevos lectores ocasionalmente pero no es probable que activen nuevos lectores tan a menudo como cada día o cada semana. Para posibilitar estos usos legítimos del sistema de activación, mientras se evita el abuso, el número de activaciones para un usuario dado (un ID de Passport™) se aumentará periódicamente, hasta un máximo definido (que será, por ejemplo, cinco activaciones inicialmente). A medida que el usuario activa nuevos dispositivos, su cuota de activaciones disponible se reduce. A medida que pasa el tiempo, el número se aumenta, a una frecuencia sugerida de, por ejemplo, una activación adicional cada 90 días (desde la fecha de la primera activación) hasta que el número alcance 10. Este tipo de límite permitirá a los usuarios activar lectores (o reactivar, es decir, lectores antiguos en dispositivos con discos duros reformateados) con una frecuencia razonable, y resistirá el abuso del sistema por los “piratas”.

Los servidores 94 de activación hacen cumplir el límite de activaciones almacenando, en la base de datos 102 de activación, una lista de todas las activaciones que ha solicitado un ID de PASSPORT™ dado, junto con sus indicaciones de fecha. Si se realiza una solicitud de re-activación, la cuota no se ve afectada, siempre que el ID de la

máquina (por ejemplo, el número único que vincula el repositorio seguro al hardware que aloja el lector) sea el mismo (puesto que esto no daría como resultado robo, ya que el mismo PC se está activando de nuevo).

Flujo de procedimiento de comercio electrónico

Una vista general del procedimiento básico por el que se obtienen y suministran los títulos de libro electrónico en línea se describe ahora con referencia a la Figura 9. Usando un explorador o las "páginas de librería" o el lector 90 o 92, el usuario elige libro o libros mediante mecanismos que el sitio de venta minorista implementa (etapa 200). El usuario a continuación paga los títulos, si se requiere pago (etapa 202). La transacción concluye en la etapa 204 con una página de recibo (es decir, una configuración de pedido o página de "gracias") que contiene enlaces (solicitudes POST) para descargar cada título comprado (es decir, los URL que contienen la dirección del servidor 76 de contenido, más la información encriptada creada por el objeto 74 de encriptación de URL). Para copias completamente individualizadas (nivel 5), un guion del lado del cliente rellenará el cuerpo del POST con el certificado de activación, preferentemente usando el objeto COM implementado mediante el lector que obtiene el certificado de activación necesario o información relevante desde el mismo.

Tras hacer clic en cualquiera de los enlaces en la etapa 206, el explorador inicia una descarga desde los servidores 76 de contenido (mediante la DLL 78 de ISAPI de servidor de descarga). Para copias selladas individualmente (exlibris (por ejemplo, nivel 3)), el servidor 76 de descarga añade el nombre del consumidor a los metadatos del título y resella la clave 14A simétrica usando un nuevo troceo criptográfico resultante de los nuevos metadatos, que ahora incluye el nombre de usuario. Para copias completamente individualizadas (nivel 5) se genera una licencia y se embebe en el fichero LIT, además del exlibris que se está crenado. Esta licencia contiene la clave 14A simétrica que encriptó el fichero LIT "sellado" con la clave pública en el certificado de activación. Cuando la descarga está completa (etapa 208), el servidor 76 de descarga registra la transacción y, en el cliente, se lanza el lector automáticamente (etapa 210). El título puede moverse a una carpeta "Mi biblioteca" (por ejemplo, en un PC usando uno de los sistemas operativos MICROSOFT WINDOWS, una carpeta de este tipo puede llamarse C:\MyLibrary, y se reservaría para el almacenamiento de ficheros LIT). El libro electrónico se abre a su página de cubierta y se presenta el nombre del propietario legítimo 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 POST a la DLL 78 de ISAPI de servidor de descarga. El cuerpo de esta solicitud post contendrá, como mínimo, el objeto binario grande encriptado generado mediante el objeto 74 de encriptación de URL. Para copias completamente individualizadas (protegidas de nivel 5) esta solicitud post contendrá también el certificado de activación requerido cuando se sella la licencia de XrML (véase a continuación).

Durante la etapa 2, la ISAPI 78 extrae, desde el cuerpo del POST, el ID del vendedor, que se requiere para capturar la clave 75 simétrica asociada con este vendedor para desencriptar el URL. A continuación desencripta y valida la solicitud de descarga. Si la solicitud es inválida y/o el TTL calculado ha expirado (por ejemplo, un posible ataque de reproducción), el servidor de descarga puede redirigir el explorador de vuelta al sitio de librería. El sitio 71 de librería debería siempre estar encapsulado en la variable de servidor REFERRER de HTTP. Durante esta etapa, puede proporcionarse un nombre de fichero amigable opcional mediante el objeto binario grande encriptado. Esta cadena, cuando se devuelve, se usará mediante la ISAPI como el nombre de fichero cuando se descarga el título LIT al usuario final.

En la etapa 3, la ISAPI 78 para el ID de libro y el tipo de ID de libro al módulo de extensión de almacenamiento de contenido, que a continuación devuelve la localización física del fichero LIT en el almacenamiento de contenido basándose en cualquiera de una entrada de caché de memoria (si el fichero LIT que se está solicitando se ha descargado previamente) o una búsqueda en la base de datos 89 de ejecución.

En la etapa 4, si el ID de libro no se encuentra en la caché de memoria local de la ISAPI 78, el fichero LIT se recupera desde el almacenamiento 80 de contenido y se copia en la caché de memoria local de la ISAPI. Cuando la ISAPI almacena en caché los ficheros LIT localmente, quita a los ficheros LIT sus claves 14A simétricas y los almacena en un cubo de caché separado, indexados por su ID respectivo, que puede aumentar la seguridad.

En la etapa 5 la ISAPI 78 realizará algunas de estas posibles etapas de acuerdo con el nivel de DRM requerido para el fichero LIT que se está descargando:

- Si la solicitud es para un fichero de DRM de nivel 1, o el fichero LIT no está sellado en origen en el almacenamiento 80 de contenido, la ISAPI preferentemente devuelve un error, indicando que la condición de error apropiada (solicitud inválida o un título inválido en el almacenamiento de contenido, respectivamente).

Para títulos sellados de origen (nivel 2), la ISAPI devolverá el fichero al usuario final, sin procesamiento alguno hecho en el fichero. Esto es similar a descargar cualquier otro fichero estático.

Para títulos sellados individualmente (nivel 3), el nombre de usuario se insertará en un nuevo flujo en el fichero LIT, los metadatos marcados con nivel 3 (para uso mediante el cliente 90 o 92 lector), los nuevos metadatos se trocean, y la clave 14A simétrica usada para encriptar el fichero LIT se sella con el nuevo valor de troceo criptográfico

calculado.

Para títulos completamente individualizados (nivel 5), la ISAPI 78 publicará, además de generar las funciones anteriormente mencionadas para el nivel 3, una solicitud al módulo 77 de licencia, que generará un objeto binario grande de XrML de licencia, lo firmará con el certificado de centro de ejecución, lo sellará con la clave pública de activación de usuario final, y lo devolverá para embeberlo en el fichero LIT.

Para ambos niveles 3 y 5, todo el procesamiento se lleva a cabo en el espacio de memoria temporal creado durante la etapa 4. Este espacio de memoria se descartará más tarde mediante la ISAPI, cuando la descarga esté completa.

En la etapa 6 la DLL de ISAPI devuelve el fichero LIT al servidor 76 IIS para descarga. Si, durante la etapa 3, el módulo de extensión de almacenamiento de contenido devolvió una cadena de “nombre amigable”, este valor se usa en el encabezamiento de HTTP como el nombre de fichero a almacenarse en la máquina del usuario.

En la etapa 7 el fichero LIT se descarga mediante el IIS al usuario final mediante HTTP. Cuando la descarga está completa, el IIS volverá a llamar a la DLL 78 de ISAPI para notificar que la solicitud pendiente se satisfizo y la conexión se cerró. La ISAPI 78 purgará a continuación toda la memoria temporal usada durante la etapa 5.

En la etapa 8, la DLL de ISAPI 78 usará la tubería de ejecución asíncrona (mediante el cliente 86 independiente MSMQ local) para registrar la transacción en la base de datos 91 de registro para informe posterior y/o facturación. Esta tubería se usa también para invalidar entradas de caché en la memoria de la ISAPI asíncronamente, de manera que cualquier modificación al almacenamiento 80 de contenido realizada mediante la herramienta 82 de gestión de contenido provocará que la ISAPI invalide los datos almacenados en caché y repliegue al módulo 88 de extensión (y posteriormente el almacenamiento 80 de contenido) para recuperar el fichero LIT para la entrada de caché invalidada.

Una vez que se ha descargado el título de libro electrónico al cliente (después de la etapa 7), el cliente lector puede lanzarse. Esto se posibilita mediante una asociación de extensión de fichero de LIT para el lector. El lector puede mover el fichero en la carpeta de biblioteca local (por ejemplo, “C:\MyLibrary”) y abrir el libro en su página de cubierta, que para títulos de nivel 3, identifica de manera evidente al propietario por encima del nombre del autor.

Funcionalidad de gestión de contenido

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

De acuerdo con una característica de la presente invención, puede haber independencia entre el servidor 76 de descarga y los servidores 80 de almacenamiento de contenido del centro de ejecución. Cada par ID de libro/tipo de ID de libro que proviene del URL proporcionado mediante los vendedores minoristas 71 se resolverá en una ruta física a un fichero LIT mediante el módulo 88 de extensión de almacenamiento de contenido, que puede personalizarse mediante cada centro 73 de ejecución. Esto proporciona máxima flexibilidad y escalabilidad del repositorio de almacenamiento de contenido así como de la DLL 78 de ISAPI de servidor de descarga.

Una base de datos de librería (vendedor minorista) se rellena con los ID de libro generados mediante una herramienta para gestionar los ficheros LIT de un centro de datos de proveedor de contenido particular. Este procedimiento se supone que tiene lugar de manera asíncrona y mediante acuerdo contractual entre el vendedor minorista 71 y el proveedor de contenido (centro de ejecución) que aloja los servidores 76 de contenido. Estos ID se proporcionarán a la DLL 78 de ISAPI de servidor de descarga mediante el URL (en la porción encriptada del URL).

Consideraciones de diseño

Se describen a continuación esquemas ejemplares para las diversas tablas usadas en las bases de datos DAS. Los esquemas ejemplares no se han de considerar como que limitan la presente invención, ya que son posibles otros esquemas.

Base de datos de ejecución

Hay tres tablas en la base de datos de ejecución ejemplar. Incluyen una tabla Producto_DAS (DAS_Product) que contiene toda la información requerida para procesar una solicitud de descarga, una Vendedores_Minoristas_Registrados_DAS (DAS_Registered_Retailers) que contiene toda la información sobre los vendedores minoristas que están permitidos a satisfacer títulos usando esta instalación de ejecución de DAS, y una Configuración_Licenciatario_DAS (DAS_Licensor_Config) que contiene la Licencia del Licenciatario requerida proporcionada mediante Microsoft para cada Socio de instalación de DAS. No hay relaciones requeridas entre estas

tablas; sin embargo, si son necesarias las relaciones de tabla, entonces se usan los identificadores únicos de cada tabla (claves primarias).

Tabla Producto_DAS

```
(
    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”
    PriceStructur   varchar(32)   not null,          -- ejemplo “Retail”
    Currency        varchar(10)   not null,          -- ejemplo “USD”
    SecurityLevel   varchar(32)   not null,          -- ejemplo “5”
    DateUpdated     datetime null DEFAULT (getDate()), -- última hora que se actualizó fila
    DateCreated     datetime null DEFAULT (getDate())  -- hora cuando se creó fila
)
```

Tabla de vendedores minoristas de DAS_Registrados

Esta tabla contiene el ID de vendedor minorista y cadena secreta que se usa cuando se calcula la clave 75 simétrica usada para encriptar/desencriptar los URL para ejecución. Cada cadena debe coincidir con la cadena usada mediante el vendedor minorista cuando se instala el objeto COM de URL encriptado, puesto que eso es cómo se autentica cada solicitud de descarga.

```
(
    DAS_Registered_Retailers_ID  int           not null IDENTITY(1,1),
    RetailerID                   varchar(256)  not null, -- ejemplo “Vendedor minorista-111-888”
    RetailerName                 varchar(256)  not null, -- ejemplo “Barnes & Noble”
    RetailerDesc                 varchar(4096) not null, -- ejemplo “vendedor minorista de libro”
    SharedSecret                 varchar(256)  not null, -- ejemplo “Making_eBooks_Happen”
    DateUpdated                  datetime null DEFAULT (getDate()),
    DateCreated                  datetime null DEFAULT (getDate())
)
```

Tabla Configuración_Licenciatario_DAS

Esta tabla contiene los ajustes de configuración para el componente de licencia del servidor de descarga. Cuando el servidor se inicia, el certificado del licenciatario y la clave privada del licenciatario se leen de esta tabla y se usan para generar licencias de nivel 5 para ficheros LIT. Se prefiere almacenar esta información en el servidor de SQL puesto que los datos son demasiado grandes para almacenarse en el registro local del servidor de descarga, y debido a los asuntos de seguridad de que la clave privada de los vendedores minoristas puede comprometerse si se almacena en un fichero plano. Permite también cambios fáciles a los parámetros de configuración del servidor de descarga, puesto que los socios DAS únicamente tienen que modificar esta tabla en la base de datos 89 de ejecución y todos los servidores de descarga captarán el cambio (mediante el componente de tubería y mensajería de ejecución asíncrona), que simplifica la gestión.

```
(
    DAS_Licensor_Config_ID  int           not null IDENTITY(1,1),
    LicensorCertificate     varchar(4096) not null, -- certificado del licenciatario firmado
    LicensorPrivateKey      varbinary(350) not null, -- formulario binario de la clave
                                                     privada del licenciatario
    DateUpdated             datetime null DEFAULT (getDate()),
    DateCreated             datetime null DEFAULT (getDate())
)
```

Base de datos de registro

La base de datos 91 de registro se usa para registrar todas las solicitudes de descarga. A medida que los servidores de descarga procesan solicitudes, la tubería de ejecución asíncrona (basándose en el Servidor de MICROSOFT® Message Queue) se usa para escribir, mediante un objeto COM residente en el servidor de base de datos de ejecución, cada mensaje desde la cola en la tabla Registro_DAS (DAS_Log). Esto permitirá que los sitios DAS auditen su ejecución, y determinen cuántas descargas tuvieron lugar, y cuándo, y cuáles son los títulos más frecuentemente descargados, etc. Esta tabla puede usarse también para fines de facturación. La base de datos de registro comprende una única tabla (Registro_DAS) que contiene todas las grabaciones de registro de transacción desde los 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,	-- únicamente 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 $”
DownloadAgent	varchar(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 102 de activación aloja toda la información requerida para activar lectores así como información de configuración para operar los servidores de activación. Hay cinco tablas en la base de datos de activación. La tabla Pares_de_Claves (Key_Pairs) soporta los pares de claves usados cuando se generan certificados de activación. La tabla Usuarios (Users) aloja los credenciales de PASSPORT™ para cada usuario activado, junto con el ID de par de claves (enlace en la tabla de Pares_de_Claves) y fecha de la primera activación. Los Dispositivos_de_Usuario (UsersDevices) es una lista de todos los ID de hardware (es decir, ID de máquina) activados por todos los usuarios. Para identificar qué máquina se está haciendo referencia, esta tabla tiene una restricción de clave primaria en Número_de_Usuario (UserNum) (una representación interna de cada usuario en la tabla Usuarios) e ID_de_máquina (MachID) (el ID de máquina calculado). La tabla_par_de_claves (KeyPtr) rastrea el número de pares de claves usados desde la tabla Pares_de_claves. Apunta también al siguiente par de claves disponible a usarse. La Configuración_AS_DB (AS_DB_Config) soporta elementos de configuración para la base de datos y los servidores 94 de activación.

Tabla Pares_de_claves

(

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), /* enlace a Dispositivos_de_Usuario.ID_de_dispositivo_De_ usuarios */
DateAssigned	Smalldatetime	null DEFAULT (NULL),
DateCreated	smalldatetime	null DEFAULT (getDate())

(continuación)

)

Tabla de usuarios

(

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 dispositivos de usuario

(

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 par_de_claves

(

NextKeyToUse	int	not null

)

Tabla de Configuración AS_DB

(

/* cuando número de claves libres cae por debajo de este número un trabajo GenKey planificado añade claves */

MinKeysAvailable int not null,

/* usuario inicialmente pude activar estos muchos PC */

MaxPCperUser int not null,

/* si usuario alcanzó el límite anterior, pero este periodo ha transcurrido desde su última Activación, usuario puede añadir uno más */

GrantExtraPCPeriodInDays int not null,

/* para evitar ataques de DOS (denegación de servicio) por re-activación del mismo PC una y otra vez, esto puede establecerse en producción aun valor bajo (por ejemplo, 3) pero la prueba puede establecerse a alto para pruebas de estrés */

MaxSamePCregistrations int not null

)

Almacenamiento de DRM en ficheros LIT

Cada fichero LIT es en efecto un pequeño sistema de ficheros, que consiste en una colección de elementos de almacenamiento y sus flujos asociados. En la raíz de cada fichero LIT está un objeto de almacenamiento especializado para DRM. Los sub-flujos del objeto de almacenamiento de DRM variarán dependiendo del nivel de DMR mediante el cual se distribuyó el fichero LIT. En un fichero LIT protegido de nivel 5, un almacenamiento de datos contiene el contenido real del libro electrónico y un almacenamiento de almacenamiento_de_DRM

(DRMStorage) contiene todos los datos binarios específicos de DRM. El almacenamiento de almacenamiento_de_DRM incluirá los flujos de flujo_de_validación (ValidationStream), flujo_de_DRM (DRMSource), y Sellado_de_DRM (DRMSealed) (para copias de origen y selladas individualmente). Para títulos completamente individualizados, el fichero LIT incluirá también el flujo de licencias, que incluye una licencia de usuario final (EUL).

Formato de licencia

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

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

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

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

               Un capítulo, y una imagen con valor de resumen

            ================================================
              ======

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

          - <!-- ================================================
            -->
          - <!-- Licenciatario del libro
            -->
          - <!-- ================================================
            -->
```

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

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

Estructura de la etiqueta BODY

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

```
- <BODY type="LICENSE" version="2.0">
    <ISSUED>2000-01-27T15:30</ISSUED>
  - <DESCRIPTOR>
    - <OBJECT type="self-proving-EUL">
        <ID type="MS-GUID">7BD394EA-C841-434d-
          A33F-5456D5E2AAAE</ID>
      </OBJECT>
    </DESCRIPTOR>
  - <!-- ========================================== -->
  - <!-- Libro con licencia                          --
    >
  - <!-- ========================================== -->
  - <WORK>
    - <OBJECT type="BOOK-LIT-FORMAT">
        <ID type="ISBN">8374-39384-38472</ID>
        <NAME>A book of James</NAME>
      </OBJECT>
      <CREATOR type="author">James the
        first</CREATOR>
      <CREATOR type="author">James the
        second</CREATOR>
    - <OWNER>
      - <OBJECT type="Person">
          <ID type="US-SSN">103-74-8843</ID>
          <NAME>Mike the man</NAME>
          <ADDRESS
            type="email">mike@man.com</ADDRE
            SS>
        </OBJECT>
      - <PUBLICKEY>
          <ALGORITHM>RSA-512</ALGORITHM>
        - <PARAMETER name="public exponent">
```

```
        <VALUE
          encoding="integer32">65537</VAL
          UE>
      </PARAMETER>
    - <PARAMETER name="modulus">
        <VALUE encoding="base64"
          size="512">u+aEb/WqgyO+aDjgYL
          xwrktqFDR4HZeIeR1g+G5vmKNZRt
          9FH4ouePWz/AJYnn2NdxoJ6mcIIAQ
          Ve6Droj2fxA==</VALUE>
      </PARAMETER>
    </PUBLICKEY>
  </OWNER>
- <!-- ============================================-->
- <!-- Componentes del libro
    -->
- <!-- Un capítulo, y una imagen con valor de resumen -->
- <!-- ============================================-->
- <PARTS>
  - <WORK>
    - <OBJECT type="Chapter">
        <ID type="relative">0</ID>
        <NAME>Chapter 1</NAME>
      </OBJECT>
    </WORK>
  - <WORK>
    - <OBJECT type="Image">
        <ID type="relative">1</ID>
        <NAME>Image 1: Photon Celebshots
          Dogs</NAME>
      </OBJECT>
    - <DIGEST sourcedata="LicensorMeta">
        <ALGORITHM>SHA1</ALGORITHM>
      - <PARAMETER name="codingtype">
```

```
            <VALUE
               encoding="string">surface-
               coding</VALUE>
            </PARAMETER>
            <VALUE encoding="base64"
               size="160">OtSrhD5GrzxMeFEm8q
               4pQICKWHI=</VALUE>
         </DIGEST>
      </WORK>
   </PARTS>
- <!-- ============================================-->
- <!-- Derechos de uso del libro                   --
   >
- <!-- ============================================-->
- <RIGHTSGROUP name="Main Rights">
      <DESCRIPTION>Some desc</DESCRIPTION>
   - <BUNDLE>
      - <TIME>
            <FROM time="2000-01-27T15:30" />
            <UNTIL time="2000-01-27T15:30" />
         </TIME>
      - <ACCESS>
         - <PRINCIPAL sequence="2">
            - <ENABLINGBITS type="sealed-
                  des-key">
                  <VALUE encoding="base64"
                     size="512">lnHtn/t2dp3u
                     +ZqLkbd7MK0K4xR4YdSX
                     aEvuk2Loh9ZRJEcPzCw+x
                     M7zbPrJb6ESj70+B2fWTcx
                     xDD+6WUB/Lw==</VALU
                     E>
               </ENABLINGBITS>
            </PRINCIPAL>
         </ACCESS>
      </BUNDLE>
```

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

```
- <PRINT maxcount="5">
  - <FEE>
    - <MONETARY>
      - <PERUSE value="5.00">
          <CURRENCY iso-
            code="USD" />
        </PERUSE>
      - <ACCOUNT>
          <ACCOUNTFROM
            id="BA-0234-
            0928392" />
          <HOUSE id="XYZ"
            url="http://somehous
            e.com/payme.asp" />
        </ACCOUNT>
    </MONETARY>
  </FEE>
  - <TRACK>
      <PROVIDERNAME>e-
        tracker</PROVIDERNAME>
      <PROVIDERID id="US1023"
        type="Tracker ID" />
    - <PARAMETER name="tracking
        address">
        <VALUE
          encoding="url">"http://so
          metrackingservice/trackm
          e.asp"></VALUE>
      </PARAMETER>
    - <PARAMETER name="tracking
        support address">
        <VALUE
          encoding="url">"http://so
          metrackingservice/support
          me.asp"></VALUE>
      </PARAMETER>
```

```
            </TRACK>
          - <TERRITORY>
              <LOCATION country="us"
                state="CA" city="El Segundo"
                postalcode="90245" />
              <LOCATION country="jp" />
            </TERRITORY>
          </PRINT>
        </RIGHTSLIST>
      </RIGHTSGROUP>
    </WORK>
  - <!--=============================================-->
  - <!-- Licenciatario del libro                     -->
  - <!--=============================================-->
  - <LICENSOR>
    - <OBJECT type="Principal-Certificate">
        <ID type="MS-GUID">7BD394EA-C841-434d-
          A33F-5456D5E2AAAE</ID>
        <NAME>Barnes and Noble</NAME>
      </OBJECT>
    - <PUBLICKEY>
        <ALGORITHM>RSA-512</ALGORITHM>
      - <PARAMETER name="public exponent">
          <VALUE
            encoding="integer32">65537</VALUE>
        </PARAMETER>
      - <PARAMETER name="modulus">
          <VALUE encoding="base64"
            size="512">u+aEb/WqgyO+aDjgYLxwrk
            tqFDR4HZeIeR1g+G5vmKNZRt9FH4oueP
            Wz/AJYnn2NdxoJ6mcIIAQVe6Droj2fxA=
            =</VALUE>
        </PARAMETER>
      </PUBLICKEY>
    </LICENSOR>
```

```
- <!-- ============================================ -->
- <!-- Licencias del libro                          -->
- <!-- ============================================ -->
- <LICENSEDPRINCIPALS>
  - <PRINCIPAL>
    - <OBJECT type="program">
        <ID
          type="msprogid">XrML.interpreter</ID
          >
        <NAME>DRPL INTERPRETER</NAME>
      </OBJECT>
    - <AUTHENTICATOR type="drm-module-
        verifier">
        <ID type="microsoft-
          progid">ms.drm.authenticode</ID>
        <NAME>DRMAuthenticode</NAME>
      - <AUTHENTICATIONCLASS>
          <VERSIONSPAN min="2.0" max="3.4"
            />
          <VERSION>5.0</VERSION>

            <SECURITYLEVEL>5</SECURITYLE
            VEL>
        </AUTHENTICATIONCLASS>
      - <VERIFICATIONDATA type="signature-
          key">
        - <PUBLICKEY>
            <ALGORITHM>RSA-
              512</ALGORITHM>
          - <PARAMETER name="public
              exponent">
              <VALUE
                encoding="integer32">65
                537</VALUE>
            </PARAMETER>
          - <PARAMETER name="modulus">
```

```
                <VALUE encoding="base64"
                  size="512">u+aEb/Wqgy
                  O+aDjgYLxwrktqFDR4HZe
                  IeR1g+G5vmKNZRt9FH4o
                  uePWz/AJYnn2NdxoJ6mcII
                  AQVe6Droj2fxA==</VALU
                  E>
              </PARAMETER>
            </PUBLICKEY>
          </VERIFICATIONDATA>
        </AUTHENTICATOR>
      </PRINCIPAL>
- <PRINCIPAL>
  - <OBJECT type="MS Ebook Device">
      <ID type="INTEL SN">Intel PII 92840-
        AA9-39849-00</ID>
      <NAME>Johns Computer</NAME>
    </OBJECT>
  - <AUTHENTICATOR type="drminternal-
      certverify-program">
      <ID type="microsoft-progid">2323-2324-
        abcd-93a1</ID>
    - <AUTHENTICATIONCLASS>
        <VERSION>1.x-2.5</VERSION>
      </AUTHENTICATIONCLASS>
    - <VERIFICATIONDATA type="authenticode-
        named-root">
      - <PUBLICKEY>
          <ALGORITHM>RSA-
            512</ALGORITHM>
        - <PARAMETER name="public
            exponent">
            <VALUE
              encoding="integer32">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>MS Book Reader 2.0</NAME>
  </OBJECT>
- <AUTHENTICATOR type="drminternal-digest-
    program">
    <ID type="microsoft-progid">2323-2324-
      abcd-93a1</ID>
  - <AUTHENTICATIONCLASS>
      <VERSION>1.x-2.5</VERSION>
    </AUTHENTICATIONCLASS>
  - <VERIFICATIONDATA type="authenticode-
      named-root">
    - <DIGEST>

        <ALGORITHM>MD5</ALGORIT
        HM>
      <VALUE encoding="base64"
        size="90">bXlwYXNzd29yZA=
        =</VALUE>
      </DIGEST>
    </VERIFICATIONDATA>
  </AUTHENTICATOR>
</PRINCIPAL>
</LICENSEDPRINCIPALS>
</BODY>
```

Autenticidad de licencia

Como se ha mencionado anteriormente, el repositorio seguro del lector autentica una licencia mediante las etiquetas SIGNATURE y DIGEST. Esto es de manera que el software de cliente puede validar que el contenido que se está presentando proviene de una fuente confiable. Se proporciona a continuación un ejemplo más detallado de estas etiquetas:

```
- <!-- ═══════════════════════════════════════════
```

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
      +NBF0eNa7de+1D6n+MPJa3J7ki8Dmwmuu/pBciQ
      nJ4xGaqRZ5AYoWRQ==</VALUE>
</SIGNATURE>
```

Escenarios de orígenes de contenido de sistema de DRM

El contenido de origen se distribuye preferentemente en un formato de libro electrónico abierto ("OEB"), que se personalizará más tarde por el vendedor minorista a cada lector de destino. El formato de OEB se especifica en el documento titulado Open eBook™ Publication Structure 1.0, con fecha de 16 de septiembre de 1999, que está disponible en http://www.openebook.org/specification.htm y se incorpora expresamente en el presente documento por referencia en su totalidad.

Escenarios de orígenes de contenido

Dentro del contexto del sistema DRM, los orígenes de contenido (autores y/o editores) de libros electrónicos se espera que proporcionen cualquiera de copias abiertas (es decir, no selladas) o selladas que estén listas para venta. Para distribuirse mediante el servidor descrito a continuación, los editores deben proporcionar copias que han sido selladas de origen como mínimo, o como alternativa, los editores pueden proporcionar opcionalmente ficheros de OEB/HTML de origen que el comerciante/distribuidor encriptará y almacenará para ejecución. Los orígenes de contenido pueden proporcionar también un fichero separado (por ejemplo, XML, texto, guion de base de datos, etc.) que proporcionará información específica de comerciante acerca de cada título que se está distribuyendo que se usará por el comerciante/distribuidor para rellenar sus bases de datos de ejecución. Tal información puede incluir el nivel de DRM deseado, precio, avance, etc.

Puesto que hay una expectativa de que se mantenga preferentemente una relación de confianza entre editores y vendedores minoristas de manera contractual y no de manera tecnológica, en general no es necesario encriptar y/o sellar títulos entre editores y comerciantes/distribuidores. Una relación de este tipo proporciona un despliegue más sencillo. Si, sin embargo, la seguridad añadida es de interés, la presente invención proporciona títulos que pueden encriptarse cuando se transfieran entre editores y comerciantes/distribuidores.

De acuerdo con la presente invención, los editores pueden distribuir el contenido a los vendedores minoristas mediante uno de suministro de medio de almacenamiento masivo portátil (CD, DVD, etc.); servidores de FTP seguros en cualquiera del sitio del editor o del comerciante/distribuidor; HTTPS seguro (SSL) en cualquiera del sitio del editor o del comerciante/distribuidor; y conexiones de red especializadas seguras entre los sitios del editor y del comerciante/distribuidor.

Escenarios de comerciante/distribuidor

Se describirán ahora varios escenarios de distribución no limitantes. Los escenarios se pretenden para proporcionar ejemplos de ventas a clientes, y no se pretende limitar la presente invención ya que son posibles otros escenarios.

Ventas de copias selladas de origen

Después de que el cliente que compra ha seleccionado los títulos que él/ella desea comprar y decide 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 ellos mismos (para aquellos que requieren un registro de afiliación de sus clientes) o simplemente rellenar un formulario de pedido. El comerciante a continuación generará y descargará un recibo (prueba de compra electrónica) al cliente que compra. Como se ha indicado anteriormente, se prefiere que el recibo electrónico incluya toda la información requerida para posibilitar al usuario descargar posteriormente los títulos que ha comprado mediante un mecanismo tal como un URL que apunta al servidor 76 de contenido y contiene el objeto binario grande encriptado generado mediante el objeto de encriptación de URL. Una vez que el usuario hace clic en el URL incluido en el recibo electrónico para descargar el título comprado, el servidor enumerado en ese URL (es decir, el servidor de ejecución o de contenido) descarga el título referenciado para el comprador. Los servidores 76 de contenido/descarga pueden validar que el pedido de hecho se realizó mediante el usuario que intentaba descargar el título.

Como se ha mencionado anteriormente, las copias selladas de origen pueden incluir indebidamente 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 herramientas para encriptar el título con una clave 14A simétrica proporcionada mediante estas herramientas. Estas mismas herramientas encriptarán la clave 14A simétrica con un troceo criptográfico de los metadatos del título y embeben la clave 14A simétrica encriptada en un flujo separado en el título. Cuando el software lector abre estos títulos, aplicará el mismo algoritmo usado mediante la herramienta para desencriptar la clave simétrica y a continuación usarla para desencriptar el contenido. Se observa que los títulos comprados de esta manera pueden volverse a distribuir fácilmente por los usuarios finales (por ejemplo, publicando el fichero LIT en la Web, o grabándolo en el disco 29 magnético o en el disco 31 óptico y enviando el disco a otro usuario); por lo tanto se recomienda que el comerciante proporcione advertencias con respecto a la distribución ilegal en cada recibo. Los propietarios de títulos vendidos de esta manera se ven alentados a incluir información de derechos de autor como parte de la publicación.

Ventas de copias selladas individualmente

Similar a las copias selladas de origen, las copias selladas individualmente (por ejemplo, nivel 3) requieren que el vendedor minorista nombre al propietario legítimo del título en los metadatos, y a continuación selle la clave 14A simétrica usada para encriptación/desencriptación del contenido con un nuevo troceo criptográfico de los nuevos metadatos, que ahora incluyen el nombre del propietario. Esto hace ventajosamente a los metadatos resistentes a la manipulación, puesto que cualquier intento para cambiar los metadatos (por ejemplo, eliminar el nombre del propietario legítimo de modo que el propietario legítimo pudiera distribuir las copias y escapar la detección) podría provocar que cualquier intento de desellar la clave 14A simétrica fallara, puesto que daría como resultado el troceo criptográfico incorrecto. Sin embargo, como las copias sin firmar y sin sello, y como las copias selladas de origen, estos títulos no proporcionan ninguna protección de copia proactiva; en su lugar, las copias selladas individualmente protegen los derechos del propietario en los trabajos basándose en el efecto disuasorio que un usuario cuyo nombre está unido en la copia y que participó en la distribución ilegal de la copia podría descubrirse fácilmente.

En el escenario, el vendedor minorista generalmente proporciona el nombre del cliente, ya que aparece en su tarjeta de crédito, como un parámetro en cada URL de descarga incluido en la página/correo electrónico de recibo (es decir, prueba de compra). Esta información se usa mediante los servidores 76 de descarga durante la ejecución para añadir el nombre del usuario a los metadatos. El uso del nombre asociado con una tarjeta de crédito es preferente, puesto que suponiendo que la tarjeta de crédito no es robada, es una fuente fiable del nombre del usuario; si el nombre proporcionado por el vendedor minorista está basado en, es decir, entrada de usuario, existe un mayor peligro de que el usuario introdujera un nombre falso que no serviría para el objetivo de vincular el nombre real del usuario a la copia.

Ventas de copias firmadas

Las copias firmadas (por ejemplo, nivel 4) son títulos que incluyen una firma digital, que se proporcionó mediante el origen de contenido (autor y/o editor) en el momento en el que se generó el título. Este es el mecanismo usado para proporcionar copias autenticables, teniendo los datos en el fichero LIT (o una porción de los mismos) firmados por diversas entidades en la cadena de distribución. El Nivel 4 puede combinarse con otros niveles - por ejemplo, es posible combinar firma de origen con cualquiera de individualización de nivel 3 o de nivel 5 para crear un título que es tanto autenticable como resistente a copia (o, en el caso del nivel 3, “disuasorio” de copia).

Ventas de copias completamente individualizadas

Las copias completamente individualizadas se diferencian de los títulos sellados individualmente en que en el tiempo de ejecución, el comerciante/distribuidor debe siempre sellar la licencia encriptando la clave 14A simétrica a la clave pública del usuario final en el certificado de autenticación del usuario final. La autenticidad de la clave pública se confirma mediante el certificado de activación, que está firmado por los servidores 94 de activación. Un comerciante puede solicitar el certificado de activación firmado la primera vez que un consumidor particular compra cualquier título completamente individualizado. Opcionalmente, los comerciantes podrían solicitar tal certificado en cada transacción, si el usuario no tiene una afiliación u otra relación con el comerciante. El certificado de activación encriptado se proporciona a un vendedor minorista mediante un componente de cliente del sistema de DRM, que puede realizarse mediante guiones mediante cualquier página web. Este certificado está encriptado para proteger la privacidad del cliente así como para reducir el riesgo de ataques de reproducción y/o piratería informática. Se prefiere que los comerciantes almacenen el certificado de activación encriptado en sus sitios para transacciones futuras.

Los títulos vendidos como copias completamente individualizadas pueden abrirse únicamente en el lector o lectores del consumidor que compra y no pueden distribuirse abiertamente. Como parte del procedimiento de vender títulos completamente individualizados, los comerciantes pueden detectar si el lector del usuario final se ha activado, que es un requisito para descargar tales títulos. Si un comerciante detecta que un lector no está activado, el comerciante puede advertir al lector que la activación es necesaria para abrir un título completamente individualizado. En el caso donde el comerciante no almacene un certificado de activación del usuario particular, sería incluso no posible proporcionar un título completamente individualizado para ese usuario. En el caso donde el comerciante almacena el certificado de activación, el comerciante puede, por ejemplo, detectar que no se ha activado el lector instalado en el dispositivo del usuario a través del que el usuario está comprando el título (aunque ese usuario puede tener otros lectores activados), caso en el que el comerciante puede proporcionar el título al usuario, pero puede advertir al usuario que debe activar el nuevo dispositivo para usar el título en ese dispositivo (sometido, por supuesto, a cualquier límite de activaciones aplicable).

Se observa que los anteriores ejemplos se han proporcionado simplemente para el fin de explicación y no se han de interpretar de ninguna manera como limitantes de la presente invención. Aunque la invención se ha descrito con referencia a las diversas realizaciones, se entiende que las palabras que se han usado en el presente documento son palabras de descripción e ilustración, en lugar de palabras de limitaciones. Además, aunque la invención se ha descrito en el presente documento con referencia a medios, materiales y realizaciones particulares, la invención no pretende estar limitada a los detalles particulares desvelados en el presente documento; en su lugar, la invención se extiende a toda estructura, procedimiento y uso funcionalmente equivalente, tal como están dentro del alcance de las reivindicaciones adjuntas. Los expertos en la materia, que tienen el beneficio de las enseñanzas de esta memoria descriptiva, pueden efectuar numerosas modificaciones a la misma y pueden realizarse cambios sin alejarse del alcance de la invención en sus aspectos.

REIVINDICACIONES

1. Un procedimiento para proporcionar un elemento (10) de contenido electrónico, comprendiendo dicho procedimiento los actos de:

encriptar un contenido (16) electrónico con una clave (14A) simétrica;
encriptar la clave simétrica con un troceo criptográfico de metadatos (12) correspondientes;
embeber la clave simétrica encriptada en el elemento de contenido electrónico;
recibir, mediante una red, una comunicación, comprendiendo dicha comunicación un localizador de recurso uniforme y proveniente de un primer dispositivo (90) de computación, dicho localizador de recurso uniforme que tiene información que al menos identifica el elemento de contenido electrónico, incluyendo dicha información un nivel de seguridad que indica un nivel de protección requerido para el contenido electrónico, incluyéndose dicha información en dicho localizador de recurso uniforme en una forma encriptada;
desencriptar dicha información encriptada;
determinar dicho nivel de protección que el contenido electrónico va a recibir; y

cuando se determina un nivel de protección dado, proporcionar (7) dicho elemento de contenido electrónico, que contiene dicho contenido electrónico encriptado, dichos metadatos correspondientes y dicha clave simétrica encriptada, a dicho primer dispositivo de computación.

2. El procedimiento de la reivindicación 1, en el que dicho localizador de recurso uniforme se proporciona a dicho primer dispositivo de computación mediante un vendedor (71) de dicho elemento de contenido electrónico.

3. El procedimiento de la reivindicación 1, en el que dicho localizador de recurso uniforme se proporciona a dicho primer dispositivo de computación en forma de un enlace en una página web, proporcionándose dicha página web a dicho primer dispositivo de computación mediante un dispositivo (72) de computación de un sitio (71) de venta minorista remoto de dicho primer dispositivo de computación.

4. El procedimiento de la reivindicación 1, en el que dicha información comprende una identificación de dicho elemento de contenido electrónico, y en el que dicho acto de proporcionar comprende usar dicha identificación de dicho elemento de contenido electrónico para recuperar dicho elemento de contenido electrónico de entre varios elementos de contenido electrónico almacenados en un dispositivo (80) de almacenamiento.

5. El procedimiento de la reivindicación 1 para usar un dispositivo (76) de computación de un sitio (73) de ejecución para proporcionar dicho elemento de contenido electrónico a dicho primer dispositivo de computación, en el que la recepción comprende recibir dicha comunicación, en el dispositivo de computación de ejecución desde dicho primer dispositivo de computación, en el que dicho localizador de recurso uniforme comprende una dirección del dispositivo de computación de ejecución, y en el que la desencriptación comprende usar un secreto para desencriptar al menos alguna de dicha información encriptada, compartiéndose dicho secreto entre el dispositivo de computación de ejecución y un dispositivo de computación de un sitio (71) de venta minorista.

6. El procedimiento de la reivindicación 5, que comprende adicionalmente incluir al menos alguna de dicha información desencriptada en dicho elemento de contenido electrónico.

7. El procedimiento de la reivindicación 5, en el que dicho secreto comprende una clave criptográfica.

8. El procedimiento de la reivindicación 7, en el que dicha clave criptográfica comprende una clave simétrica.

9. El procedimiento de la reivindicación 1 para evitar distribución no autorizada de contenido, en el que dicha información encriptada comprende información de tiempo, y en el que la desencriptación comprende desencriptar dicha información encriptada para recuperar dicha información de tiempo, comprendiendo el procedimiento:

determinar (168), basándose en dicha información de tiempo, si ha expirado un límite de tiempo.

10. El procedimiento de la reivindicación 9, que comprende adicionalmente el acto de: cuando ha expirado el límite de tiempo, al menos denegar temporalmente dicho elemento de contenido electrónico a dicho primer dispositivo de computación.

11. El procedimiento de la reivindicación 1 o 9, en el que dicho elemento de contenido electrónico comprende información textual.

12. El procedimiento de la reivindicación 1 o 9, en el que dicho elemento de contenido electrónico comprende trabajos multimedia.

13. El procedimiento de la reivindicación 9, en el que dicha información de tiempo comprende una indicación de tiempo, y en el que dicho límite de tiempo comprende una cantidad fijada de tiempo posterior a [[el]] un tiempo especificado en dicha indicación de tiempo.

14. El procedimiento de la reivindicación 13, en el que dicha indicación de tiempo comprende el tiempo en el que se

encriptó dicha primera información encriptada.

15. El procedimiento de la reivindicación 2 que comprende los siguientes actos realizados por el vendedor:

recibir (202) un pedido para dicho elemento de contenido electrónico desde dicho primer dispositivo (90) de computación;
crear otra información relacionada con dicho elemento de contenido electrónico;
encriptar (74) dicha otra información con un secreto para producir dicha otra información encriptada, compartiéndose dicho secreto entre el vendedor y un sitio (73) de ejecución; y
transmitir (204) a dicho primer dispositivo de computación el localizador de recurso uniforme, comprendiendo dicho localizador de recurso uniforme una dirección de red de un sistema (76) de computación asociado con dicho sitio de ejecución.

16. El procedimiento de la reivindicación 15, en el que dicho secreto comprende una clave criptográfica.

17. El procedimiento de la reivindicación 1 para evitar distribución no autorizada de contenido, en el que dicha comunicación se inicia (1) en dicho primer dispositivo de computación basándose en una primera solicitud de HTTP, comprendiendo dicha primera solicitud de HTTP una dirección de un dispositivo (76) de computación de un sitio (73) de ejecución y dicha información encriptada, comprendiendo adicionalmente dicha primera solicitud de HTTP un troceo de dicha información encriptada calculada antes de la encriptación de dicha información encriptada, y en el que el procedimiento comprende adicionalmente:

determinar, basándose en una comparación del troceo calculado con la información desencriptada que dicha información encriptada no se ha manipulado.

18. El procedimiento de la reivindicación 17, que comprende adicionalmente los actos de:

recibir otra comunicación desde un segundo dispositivo (92) de computación, comprendiendo dicha otra comunicación segunda información encriptada, iniciándose dicha otra comunicación en dicho segundo dispositivo de computación basándose en una segunda solicitud de HTTP, comprendiendo dicha segunda solicitud de HTTP una dirección del dispositivo de computación de ejecución y dicha segunda información encriptada, comprendiendo adicionalmente dicha segunda solicitud de HTTP un troceo de la segunda información encriptada calculada antes de la encriptación de la segunda información;
desencriptar dicha segunda información encriptada;
determinar, basándose en una comparación de la segunda información desencriptada con el troceo de la segunda información encriptada que dicha segunda información encriptada se ha manipulado; y
al menos denegar temporalmente dicho segundo elemento de contenido electrónico a dicho segundo dispositivo de computación.

19. El procedimiento de la reivindicación 17, en el que dicha primera solicitud de HTTP comprende una solicitud POST.

20. El procedimiento de la reivindicación 17, en el que dicha primera solicitud de HTTP comprende una solicitud GET.

21. Una arquitectura (70) de servidor adaptada para suministrar (7) un elemento (10) de contenido electrónico a dispositivos (90, 92) cliente, que comprende:

medios adaptados para realizar las etapas de:

encriptar un contenido (16) electrónico con una clave (14A) simétrica;
encriptar la clave simétrica con un troceo criptográfico de metadatos (12) correspondientes; y
embeber la clave simétrica encriptada en el elemento de contenido electrónico;

y un servidor de descarga que comprende:
un módulo (78) de validación adaptado para validar solicitudes entrantes para el elemento de contenido electrónico, en el que dichas solicitudes entrantes para el elemento de contenido electrónico comprenden un localizador de recurso uniforme que comprende al menos alguna información en una forma encriptada, en el que la información al menos identifica el elemento de contenido electrónico e incluye un nivel de seguridad que indica un nivel de protección requerido para el contenido electrónico, estando adaptado adicionalmente el módulo de validación para desencriptar dicha información encriptada;
un módulo (88) de almacenamiento de contenido adaptado para determinar una localización (80) en el servidor de descarga del contenido electrónico solicitado; y
un módulo de determinación de nivel de seguridad adaptado para determinar dicho nivel de protección del contenido electrónico a recibir, en el que cuando se determina un nivel de protección dado, el elemento de contenido electrónico suministrado mediante el servidor de descarga a los dispositivos cliente contiene dicho contenido electrónico encriptado con dicha clave simétrica, dichos metadatos correspondientes y dicha clave simétrica encriptada.

22. La arquitectura de servidor de la reivindicación 21, en la que dicho módulo de validación desencripta dicha información encriptada.

23. La arquitectura de servidor de la reivindicación 22, en la que dichas solicitudes entrantes están basadas en un localizador de recurso uniforme, comprendiendo dicho localizador de recurso uniforme al menos alguna de dicha información encriptada y una dirección de dicho servidor de descarga.

FIG. 1

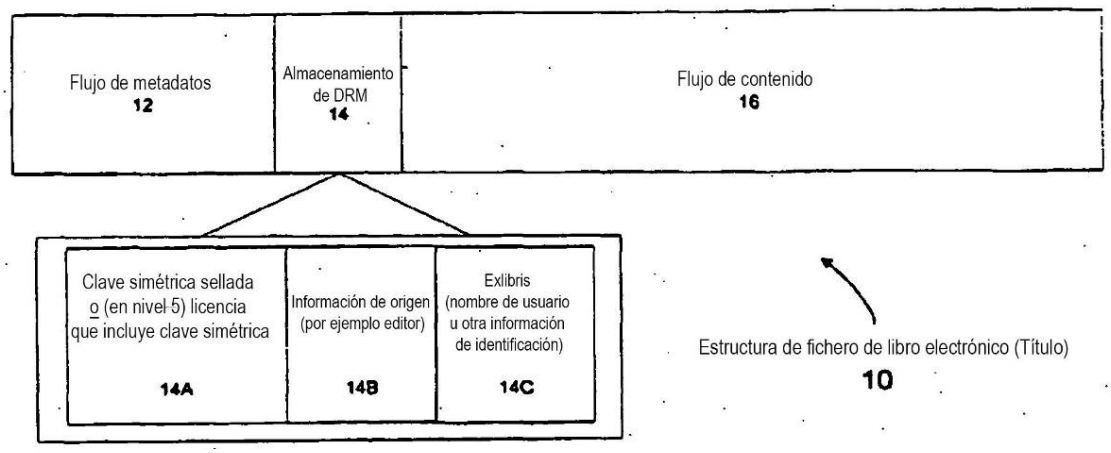
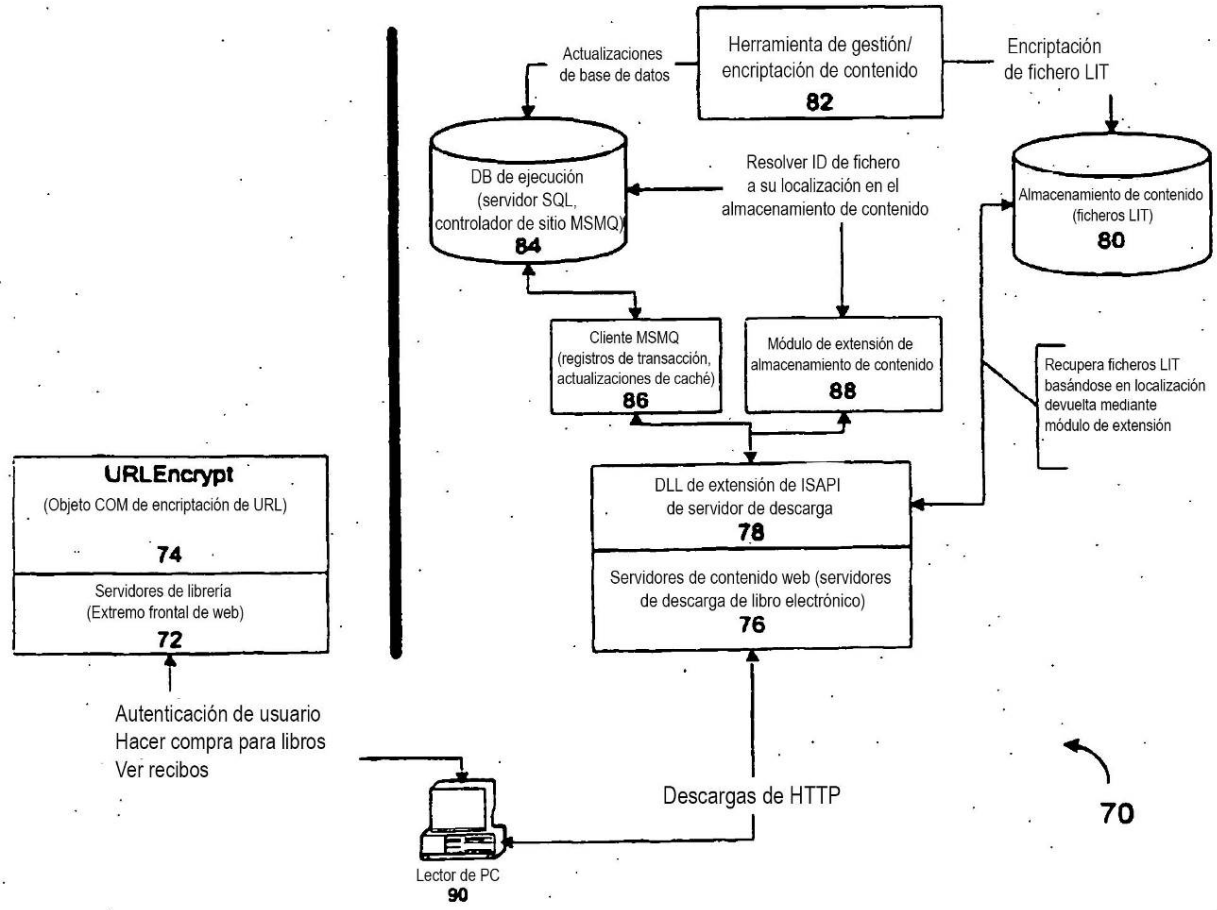

Flujo de metadatos
12
Almacenamiento de DRM
14
Flujo de contenido
16
Clave simétrica sellada o (en nivel 5) licencia que incluye clave simétrica
14A
Información de origen (por ejemplo editor)
14B
Exlibris (nombre de usuario u otra información de identificación)
14C
Estructura de fichero de libro electrónico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

FIG. 3


Actualizaciones de base de datos
Herramienta de gestión/ encriptación de contenido
82
Encriptación de fichero LIT
DB de ejecución (servidor SQL, controlador de sitio MSMQ)
84
Resolver ID de fichero a su localización en el almacenamiento de contenido
Almacenamiento de contenido (ficheros LIT)
80
Cliente MSMQ (registros de transacción, actualizaciones de caché)
86
Módulo de extensión de almacenamiento de contenido
88
Recupera ficheros LIT basándose en localización devuelta mediante módulo de extensión
URLEncrypt
(Objeto COM de encriptación de URL)
74
DLL de extensión de ISAPI de servidor de descarga
78
Servidores de contenido web (servidores de descarga de libro electrónico)
76
Servidores de librería (Extremo frontal de web)
72
Autenticación de usuario
Hacer compra para libros
Ver recibos
Descargas de HTTP
70
Lector de PC
90

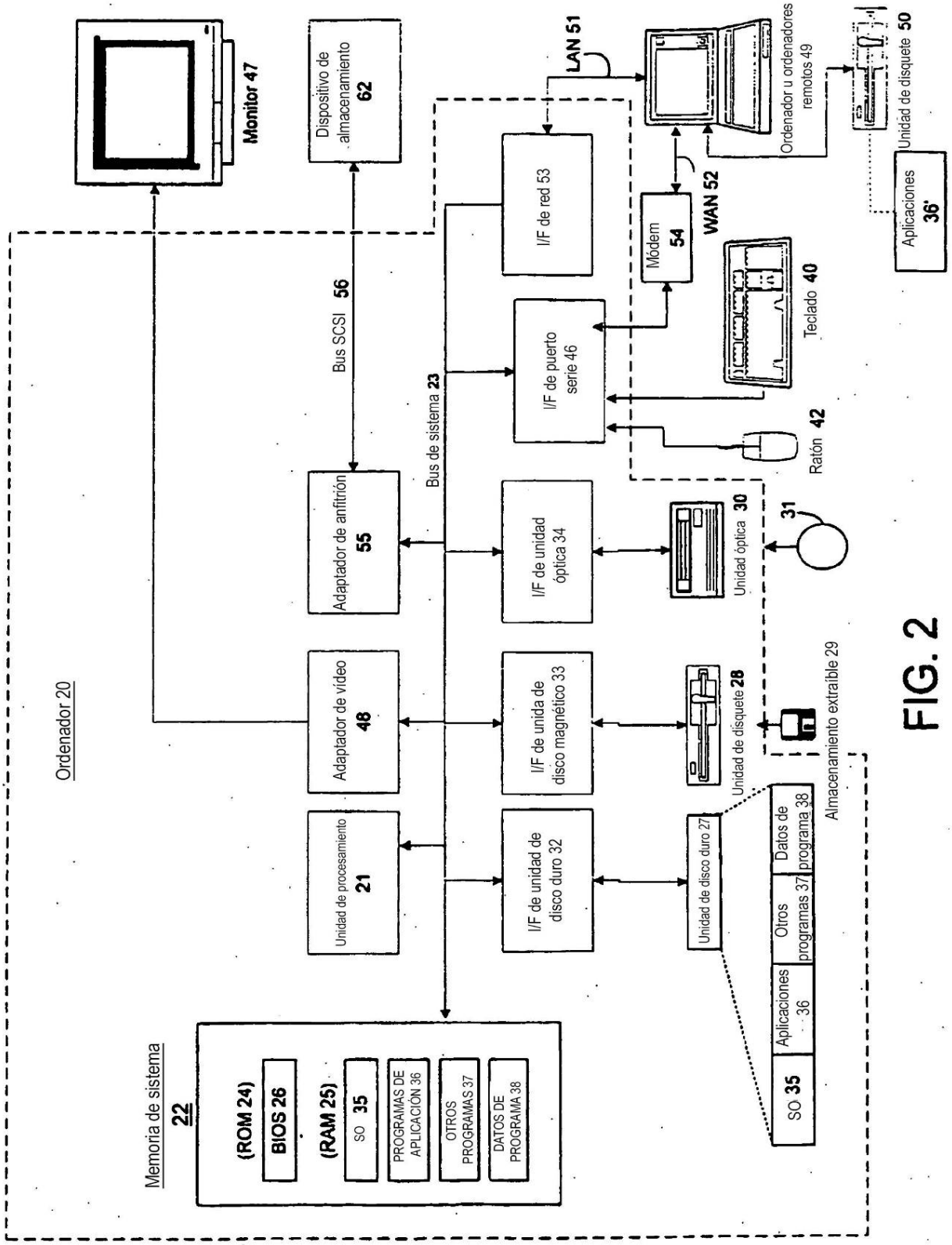

Ordenador 20
Monitor 47
Dispositivo de almacenamiento 62
LAN 51
Ordenador u ordenadores remotos 49
Unidad de disquete 50
Aplicaciones 36'
I/F de red 53
Módem 54
WAN 52
Bus SCSI 56
Bus de sistema 23
I/F de puerto serie 46
Teclado 40
Ratón 42
Adaptador de anfitrión 55
I/F de unidad óptica 34
Unidad óptica 30
31
Adaptador de vídeo 48
I/F de unida de disco magnético 33
Unidad de disquete 28
Unidad de procesamiento 21
I/F de unidad de disco duro 32
Unidad de disco duro 27
Almacenamiento extraíble 29
Memoria de sistema 22
(ROM 24)
BIOS 26
(RAM 25)
SO 35
PROGRAMAS DE APLICACIÓN 36
OTROS PROGRAMAS 37
DATOS DE PROGRAMA 38
SO 35
Aplicaciones 36
Otros programas 37
Datos de programa 38

FIG. 2

FIG. 4

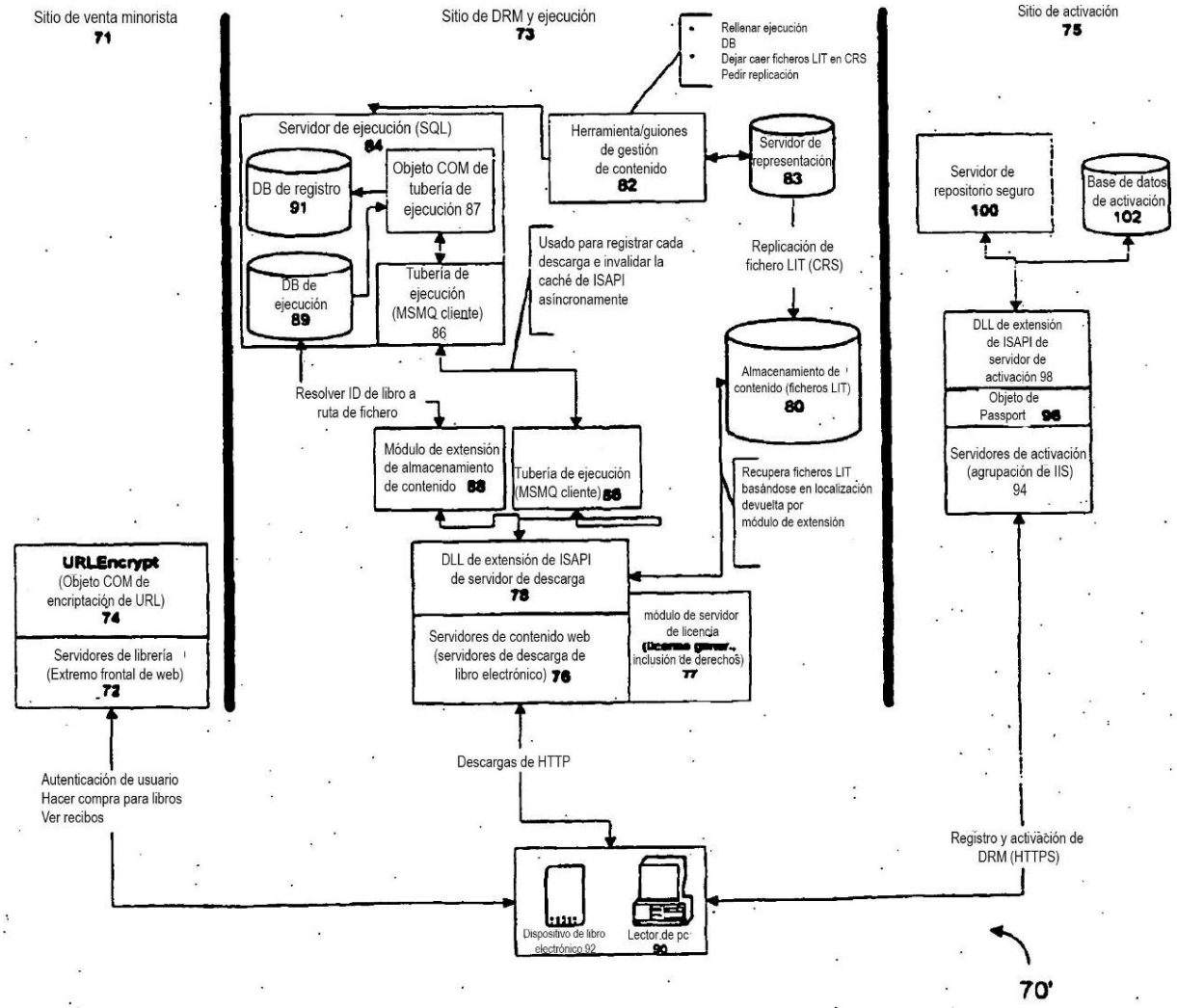

Sitio de venta minorista
71
Sitio de DRM y ejecución
73
Sitio de activación
75
Rellenar ejecución DB
Dejar caer ficheros LIT en CRS
Pedir replicación
Servidor de ejecución (SQL)
84
DB de registro
91
Objeto COM de tubería de ejecución 87
DB de ejecución
89
Tubería de ejecución (MSMQ cliente)
86
Herramienta/guiones de gestión de contenido
82
Servidor de representación
83
Usado para registrar cada descarga e invalidar la caché de ISAPI asíncronamente
Replicación de fichero 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 Passport 96
Servidores de activación (agrupación de IIS)
94
Almacenamiento de contenido (ficheros LIT)
80
Resolver ID de libro a ruta de fichero
Módulo de extensión de almacenamiento de contenido 88
Tubería de ejecución (MSMQ cliente) 86
Recupera ficheros LIT basándose en localización devuelta por módulo de extensión
URLEncrypt
(Objeto COM de encriptación de URL)
74
Servidores de librería (Extremo frontal de web)
72
DLL de extensión de ISAPI de servidor de descarga
78
Servidores de contenido web (servidores de descarga de libro electrónico) 76
módulo de servidor de licencia
(inclusión de derechos)
77
Descargas de HTTP
Autenticación de usuario
Hacer compra para libros
Ver recibos
Registro y activación de DRM (HTTPS)
Dispositivo de libro electrónico 92
Lector de pc
90
70'

FIG. 5

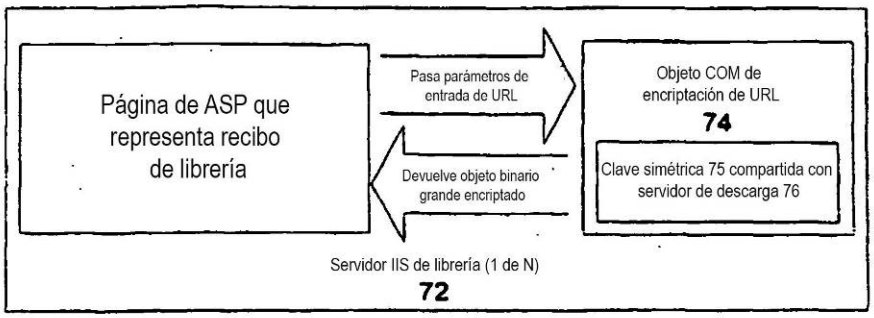

Página de ASP que representa recibo de librería
Pasa parámetros de entrada de URL
Devuelve objeto binario grande encriptado
Objeto COM de encriptación de URL
74
Clave simétrica 75 compartida con servidor de descarga 76
Servidor IIS de librería (1 de N)
72

FIG. 6

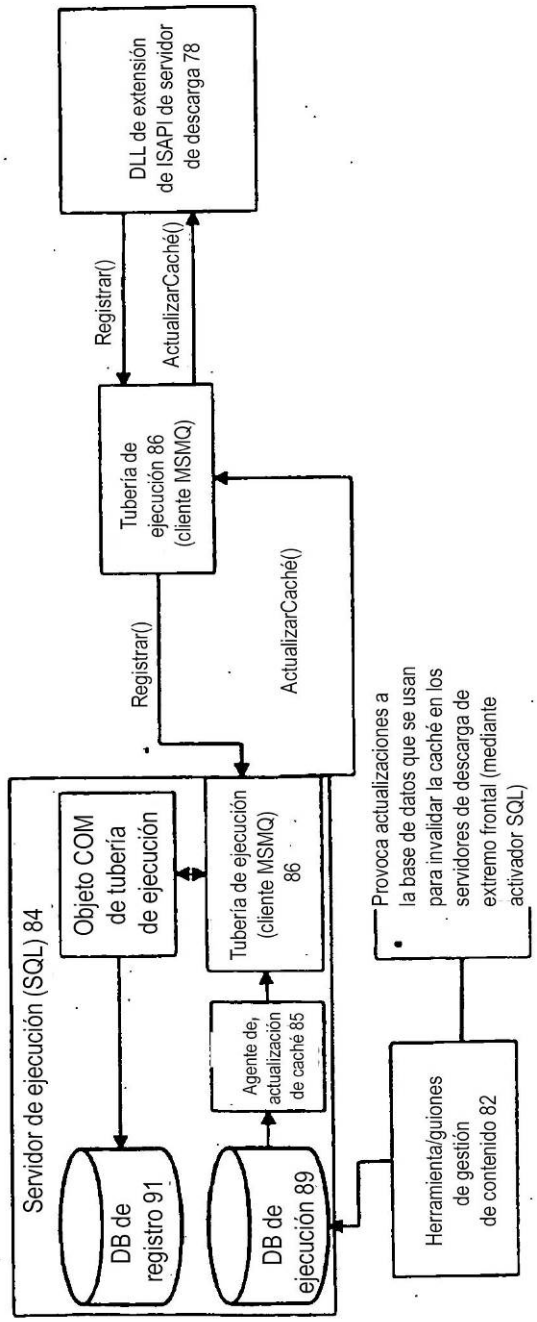

DLL de extensión de ISAPI de servidor de descarga 78
Registrar()
ActualizarCaché()
Tubería de ejecución 86 (cliente MSMQ)
Registrar()
ActualizarCaché()
Servidor de ejecución (SQL) 84
Objeto COM de tubería de ejecución
Tubería de ejecución (cliente MSMQ) 86
Agente de actualización de caché 85
DB de registro 91
DB de ejecución 89
Provoca actualizaciones a la base de datos que se usan para invalidar la caché en los servidores de descarga de extremo frontal (mediante activador SQL)
Herramienta/guiones de gestión de contenido 82

FIG. 7

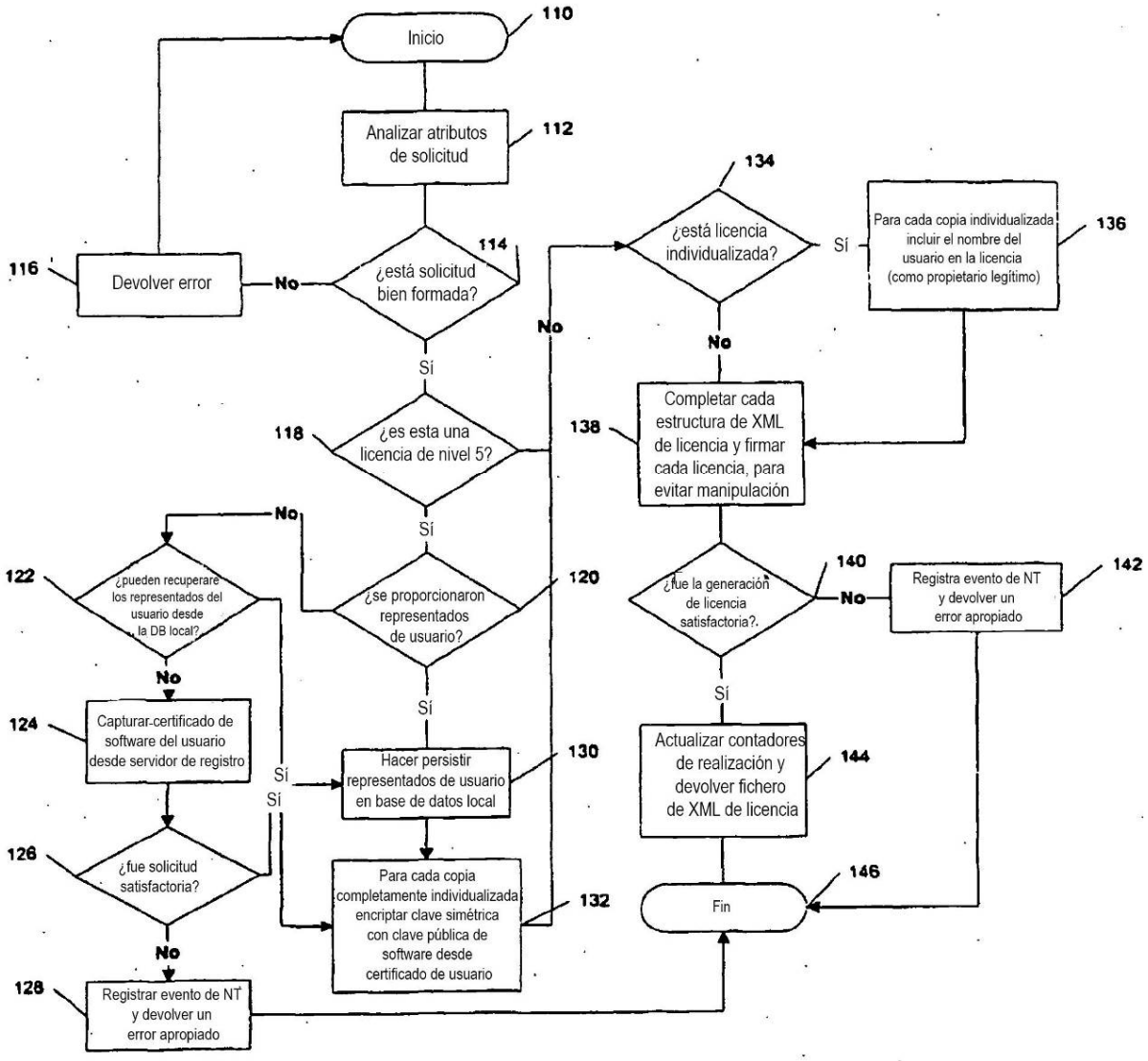

Inicio
110
Analizar atributos de solicitud
112
¿está solicitud bien formada?
114
No
Devolver error
116
Sí
¿es esta una licencia de nivel 5?
118
Sí
No
¿se proporcionaron representados de usuario?
120
Sí
No
¿pueden recuperarse los representados del usuario desde la DB local?
122
No
Capturar certificado de software del usuario desde servidor de registro
124
¿fue solicitud satisfactoria?
126
No
Registrar evento de NT y devolver un error apropiado
128
Sí
Sí
Hacer persistir representados de usuario en base de datos local
130
Para cada copia completamente individualizada encriptar clave simétrica con clave pública de software desde certificado de usuario
132
¿está licencia individualizada?
134
Sí
Para cada copia individualizada incluir el nombre del usuario en la licencia (como propietario legítimo)
136
No
No
Completar cada estructura de XML de licencia y firmar cada licencia, para evitar manipulación
138
¿fue la generación de licencia satisfactoria?
140
No
Registra evento de NT y devolver un error apropiado
142
Sí
Actualizar contadores de realización y devolver fichero de XML de licencia
144
Fin
146

FIG. 8

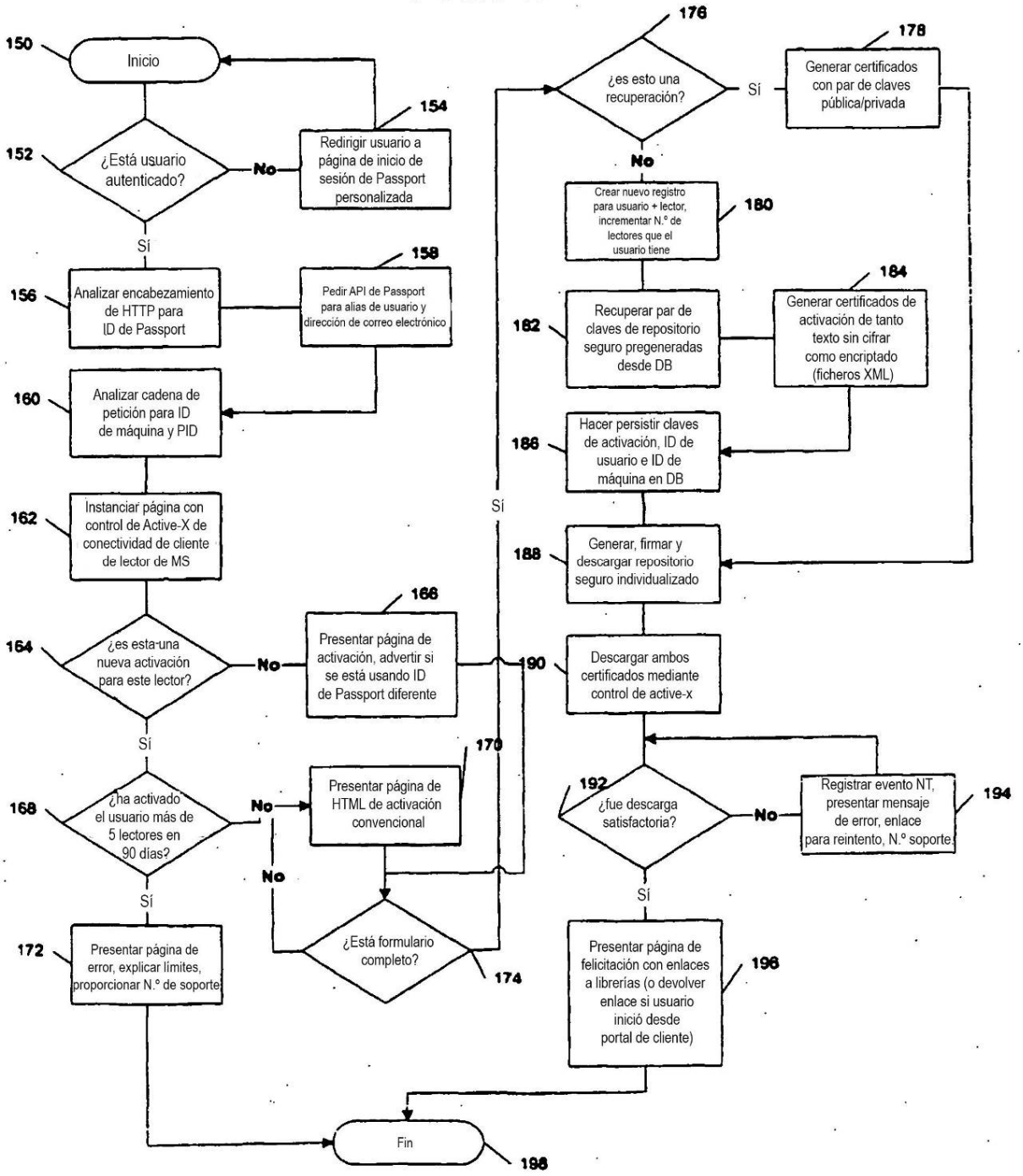

150
Inicio
152
¿Está usuario autenticado?
No
154
Redirigir usuario a página de inicio de sesión de Passport personalizada
Sí
156
Analizar encabezamiento de HTTP para ID de Passport
158
Pedir API de Passport para alias de usuario y dirección de correo electrónico
160
Analizar cadena de petición para ID de máquina y PID
162
Instanciar página con control de Active-X de conectividad de cliente de lector de MS
164
¿es esta una nueva activación para este lector?
No
166
Presentar página de activación, advertir si se está usando ID de Passport diferente
Sí
168
¿ha activado el usuario más de 5 lectores en 90 días?
No
170
Presentar página de HTML de activación convencional
Sí
172
Presentar página de error, explicar límites, proporcionar N.º de soporte
No
¿Está formulario completo?
174
Sí
176
¿es esto una recuperación?
Sí
178
Generar certificados con par de claves pública/privada
No
180
Crear nuevo registro para usuario + lector, incrementar N.º de lectores que el usuario tiene
182
Recuperar par de claves de repositorio seguro pregeneradas desde DB
184
Generar certificados de activación de tanto texto sin cifrar como encriptado (ficheros XML)
186
Hacer persistir claves de activación, ID de usuario e ID de máquina en DB
188
Generar, firmar y descargar repositorio seguro individualizado
190
Descargar ambos certificados mediante control de active-x
192
¿fue descarga satisfactoria?
No
194
Registrar evento NT, presentar mensaje de error, enlace para reintento, N.º soporte
Sí
196
Presentar página de felicitación con enlaces a librerías (o devolver enlace si usuario inició desde portal de cliente)
Fin
198

FIG. 9

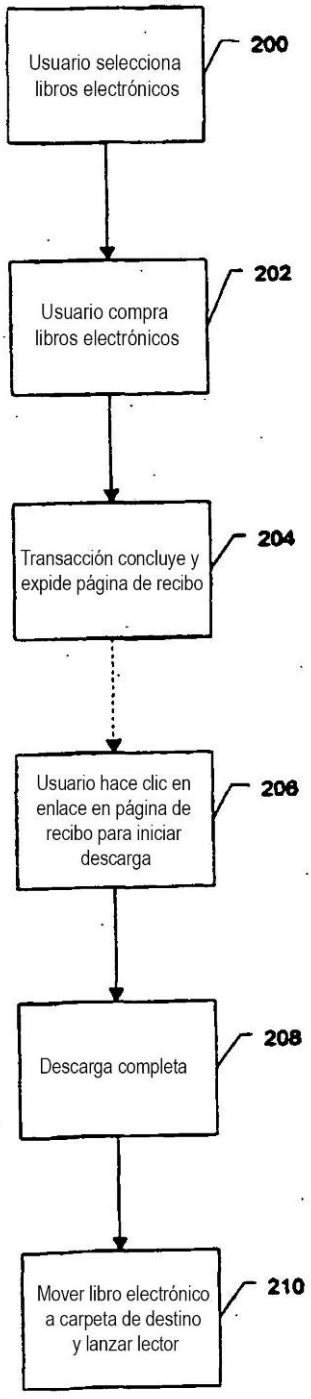
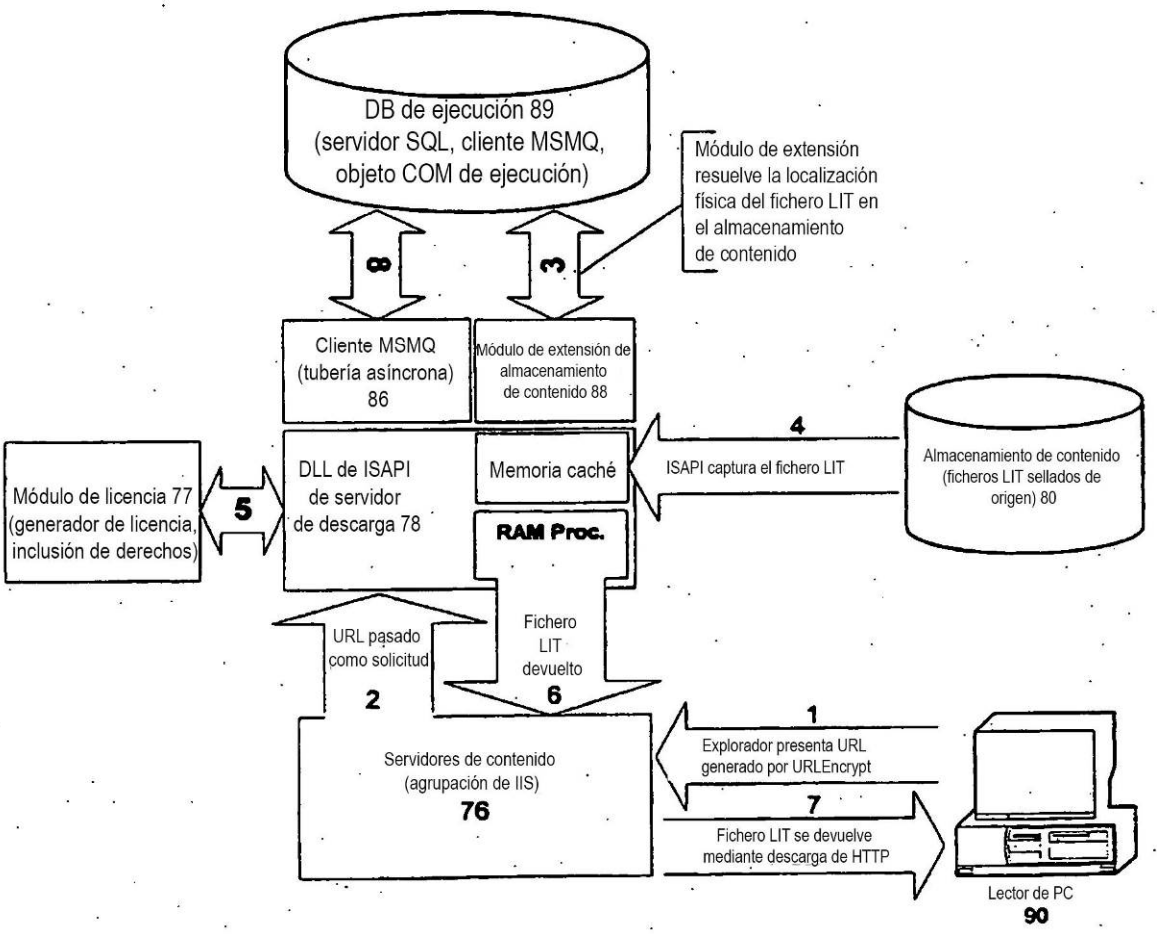

Usuario selecciona libros electrónicos
200
Usuario compra libros electrónicos
202
Transacción concluye y expide página de recibo
204
Usuario hace clic en enlace en página de recibo para iniciar descarga
206
Descarga completa
208
Mover libro electrónico a carpeta de destino y lanzar lector
210

FIG. 10


DB de ejecución 89
(servidor SQL, cliente MSMQ,
objeto COM de ejecución)
Módulo de extensión
resuelve la localización
física del fichero LIT en
el almacenamiento
de contenido
8
3
Cliente MSMQ
(tubería asíncrona)
86
Módulo de extensión de
almacenamiento
de contenido 88
4
Módulo de licencia 77
(generador de licencia,
inclusión de derechos)
5
DLL de ISAPI
de servidor
de descarga 78
Memoria caché
ISAPI captura el fichero LIT
Almacenamiento de contenido
(ficheros LIT sellados de
origen) 80
RAM Proc.
URL pasado
como solicitud
2
Fichero
LIT
devuelto
6
1
Explorador presenta URL
generado por URLEncrypt
Servidores de contenido
(agrupación de IIS)
76
7
Fichero LIT se devuelve
mediante descarga de HTTP
Lector de PC
90