(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 625 939**

(51) Int. CI.:

G06F 21/00 (2013.01)
G06F 15/16 (2006.01)
G06F 17/00 (2006.01)
H04L 9/14 (2006.01)
G06F 3/00 (2006.01)
G11B 20/10 (2006.01)
G06F 21/10 (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **25.06.2009 PCT/US2009/048710**

(87) Fecha y número de publicación internacional: **30.12.2009 WO09158531**

(96) Fecha de presentación y número de la solicitud europea: **25.06.2009 E 09771063 (6)**

(97) Fecha y número de publicación de la concesión europea: **08.03.2017 EP 2316095**

(54) Título: **Concesión de licencias de contenido protegido para conjuntos de aplicaciones**

(30) Prioridad:

27.06.2008 US 163548

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
21.07.2017

(73) Titular/es:

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

(72) Inventor/es:

RAY, KENNETH, D.;
KAMAT, PANKAJ, M.;
KAUFMAN, CHARLES, W.;
LEACH, PAUL, J.;
TIPTON, WILLIAM, R.;
HERRON, ANDREW;
KARAMFILOV, KRASSIMIR, E.;
BRYCE, DUCAN, G.;
SCHWARTZ, JONATHAN, D.;
SETZER, MATTHEW, C. y
MCDOWELL, JOHN

(74) Agente/Representante:

CARPINTERO LÓPEZ, Mario

DESCRIPCIÓN

Concesión de licencias de contenido protegido para conjuntos de aplicaciones

Los sistemas informáticos y la tecnología relacionada afectan a muchos aspectos de la sociedad. De hecho, la capacidad del sistema informático de procesar información ha transformado la forma en la que viven y trabajan los seres humanos. En la actualidad, los sistemas informáticos realizan comúnmente una serie de tareas (por ejemplo, procesamiento de textos, programación, contabilidad, etc.) que se realizaban de forma manual antes de la aparición del sistema informático. Más recientemente, los sistemas informáticos se han acoplado unos con otros y con otros dispositivos electrónicos para formar redes informáticas tanto cableadas como inalámbricas a través de las cuales pueden transferir contenido electrónico los sistemas informáticos y otros dispositivos electrónicos. Por consiguiente, la ejecución de muchas tareas de computación está distribuida a través de un número de diferentes sistemas informáticos y / o un número de diferentes entornos de computación.

Sin embargo, a pesar de que el contenido electrónico puede ser accesible para un número de sistemas informáticos, el creador del contenido electrónico puede desear limitar el acceso a los datos electrónicos. En algunos entornos, uno o más mecanismos de acceso, tales como, por ejemplo, protección de contraseñas, establecimiento de atributos de archivo, (por ejemplo, solo lectura, etc.), cortafuegos, etc., se pueden usar para limitar el acceso a un contenido electrónico. En esencia, estos mecanismos proporcionan el mismo nivel de acceso al contenido electrónico a cualquiera que esté autorizado. No obstante, si un usuario puede acceder a un archivo, por lo general no hay limitación alguna acerca de qué puede hacer eso con los contenidos de un archivo. Por ejemplo, si un usuario puede leer un archivo, el usuario puede copiar los contenidos del archivo en otra ubicación en la que otros pueden ser capaces de acceder al archivo, el usuario puede imprimir el archivo y dejar una copia en formato impreso en alguna parte, etc., por lo general sin limitación alguna.

Como resultado, en algunos entornos, un creador de un contenido electrónico puede desear un control de acceso más configurable y / o granular para su contenido electrónico. En estos otros entornos, un creador de contenidos puede usar la Gestión de Derechos Digitales (“DRM”, *Digital Rights Management*) para controlar el acceso a su contenido electrónico. En general, la DRM incluye tecnologías de control de acceso que son usadas por los creadores de contenidos para limitar el uso de contenido electrónico (o de instancias del mismo). Por lo tanto, se han desarrollado diversos tipos diferentes de DRM para proteger diferentes tipos de contenido electrónico, tales como, por ejemplo, imágenes, películas, vídeos, música, programas, multimedia, juegos, documentos, etc.

Una categoría de DRM, la Gestión de Derechos Empresariales (“ERM”, *Enterprise Rights Management*), se usa a menudo para controlar el acceso a documentos, tales como, por ejemplo, mensajes de correo electrónico, documentos de procesamiento de textos y páginas Web, etc. Servicios de Gestión de Derechos (“RMS”, *Rights Management Services*) es una solución de ERM. El RMS se puede usar para cifrar documentos, y a través de directivas basadas en servidor, evitar que los documentos sean descifrados excepto por personas o grupos especificados, en determinados entornos, en determinadas condiciones, y durante determinados periodos de tiempo. Operaciones basadas en documentos como impresión, copia, edición, reenvío y borrado se pueden permitir o no permitir para documentos individuales. Los administradores de RMS pueden implementar plantillas de RMS que agrupan estos derechos conjuntamente en unas directivas previamente definidas que se pueden aplicar en masa al contenido.

Por consiguiente, un contenido protegido por RMS puede ser creado por aplicaciones habilitadas para RMS. El contenido protegido por RMS está cifrado y puede contener una directiva de uso incrustada, que define los derechos que tiene cada usuario o grupo sobre el contenido. Un sistema de RMS funciona mediante la asignación de derechos a entidades de confianza, que son o bien usuarios individuales o bien grupos de usuarios. Los derechos se asignan en función de la entidad. El RMS define y reconoce diversos derechos por defecto - tales como permiso para leer, copiar, imprimir, guardar, reenviar y editar - y se puede extender a reconocer derechos adicionales (que tendría que implementar de forma explícita cada aplicación).

En general, para proteger un contenido, un autor de contenidos especifica una licencia de publicación (“PL”, *publishing license*) que se ha de aplicar al contenido. La licencia de publicación contiene la totalidad de la información relevante de control de acceso y de restricción de uso para proteger el contenido. Entonces, el autor de contenidos emite el contenido y la PL a una aplicación habilitada para RMS que aplica la información de control de acceso y de restricción de uso al contenido. Cuando un usuario solicita acceso al contenido, la información de control de acceso y de restricción de uso se evalúa para determinar los derechos de acceso para el usuario.

En un primer momento, un usuario puede emitir una información de autenticación a un servidor de RMS para probar su identidad. Posteriormente, el servidor de RMS puede comprobar la información de control de acceso y de restricción de uso para determinar los derechos del usuario en el contenido. Entonces, el servidor de RMS puede devolver una licencia de uso (“UL”, *use license*) que refleja el acceso permitido del usuario en el contenido.

No obstante, la seguridad en una máquina de un usuario es mantenida por un componente de RMS que no confía en otros procesos y confía solo mínimamente en el entorno de ejecución (incluyendo dlls compartidas, otro software en el sistema, depuradores de modo de usuario, etc.) que es proporcionado por el sistema operativo. Además, el

componente de RMS intenta proteger el proceso de RMS frente a ataques, tales como, depuradores de proceso, depuradores de modo de núcleo, otras aplicaciones, ataques por inyección de código, reenrutamiento de la función de Importar Tabla de Access, etc. El componente de RMS usa antidepuración, ofuscación y otras técnicas de DRM para llevar a cabo esta tarea. El componente de RMS intenta proporcionar un lugar "seguro" para evaluar la directiva y un lugar "seguro" para almacenar secretos raíz, lo que permite el almacenamiento en memoria caché de datos, posibilitando el acceso sin conexión a datos protegidos. Además, este incluye Autenticación de Módulos, que intenta validar la aplicación de llamada, su pila de llamada, etc. Las aplicaciones que usan este tipo de componente de RMS requieren un manifiesto y firma de RMS especial.

No obstante, a pesar de estar fuertemente ofuscado, el componente de RMS, en esencia, contiene un par de clave pública / privada que se usa para la comunicación con el servidor de RMS y para el almacenamiento de secretos raíz.

El acceso a los datos es protegido por la PL que se mantiene con los propios datos. La PL contiene la totalidad de la información relevante de control de acceso y de restricción de uso que protege esos datos. La PL se asocia con una criptografía de clave pública a un Servidor de RMS específico y es firmada por el certificado de licencia de cliente ("CLC", *client license certificate*) de la máquina de cliente que el servidor de RMS corporativo emitió a la máquina de cliente. Un URL para ese servidor de RMS está contenido sin cifrar en la PL de tal modo que una aplicación con reconocimiento de RMS puede hallar el servidor de RMS específico para solicitar acceso a la información protegida.

Con el fin de que la aplicación de cliente lea los datos, el componente de RMS ha de obtener, en primer lugar, un certificado de cuenta de gestión de derechos ("RAC", *rights management account certificate*), que identifica a un usuario específico. El RAC contiene una porción tanto pública como privada. Antes de que el servidor de RMS emita un RAC a una aplicación dada, en primer lugar este valida que ese entorno de seguridad local sea válido. Por lo general, esta comprobación se realiza al pedir al componente de RMS que firme con una clave privada incrustada. Esta ruta de código se basa fuertemente en la ofuscación y otras funciones y técnicas de "caja negra" solo si el entorno circundante es válido. Las infracciones tanto en la propia función como en la extracción directa de la clave privada incrustada del almacén de RSA del componente de RMS permitirían que un entorno que se ha visto comprometido engañara al servidor para que emitiera de todos modos el RAC. El RAC es protegido por la seguridad de RMS local y por las credenciales de inicio de sesión del usuario.

En segundo lugar, la aplicación de cliente ha de obtener la UL. Un cliente envía su identificación en forma de RAC al servidor de RMS, junto con la PL para el contenido que desea consumir el mismo. En respuesta, el servidor de RMS comprueba la PL para asegurar que la identidad específica que es representada por el RAC está autorizada a leer el contenido. Si está autorizada, entonces el servidor de RMS crea una UL que está cifrada para el RAC. La UL se puede almacenar en memoria caché en la máquina local para facilitar el posterior acceso sin conexión a los datos.

Desafortunadamente, la mínima confianza del componente de RMS del sistema operativo obliga a que cada aplicación de cliente desarrolle su propio procedimiento para almacenar PL junto con un contenido protegido. Las PL pueden ser de longitud variable, lo que supone una complicación adicional para la capacidad de la aplicación de cliente de almacenar PL. Por lo general, una aplicación de cliente usa su propio formato de datos para almacenar PL. Por ejemplo, una aplicación de cliente puede almacenar una PL en un encabezado en el formato de archivo, en un encabezado de paquete o mensaje adicional en una transmisión de datos protegidos, etc.

El documento US 2002/049679 A1 se refiere a un sistema y procedimiento de concesión segura de licencias de contenido digital. Cuando el usuario solicita una película, un servidor Web proporciona un URL para la ubicación de la película a un dispositivo de usuario habilitado para red (UND, *user network-enabled device*). El URL dirige la solicitud hacia un servidor de contenidos. El servidor de contenidos entregará la película solicitada en una forma cifrada al UND. Los servidores de aplicaciones están autorizados a acceder a un generador de licencias a través de un cortafuegos. El generador de licencias genera una licencia para una película solicitada por un usuario basándose en la información de reglas de negocio que es pasada al generador de licencias por los servidores de aplicaciones. Cuando un usuario en el UND solicita una licencia para un contenido, se proporciona un bloque de información de solicitud de licencia 303 al sitio Web principal. El bloque de información de solicitud de licencia 303 puede incluir una información acerca del modelo de alquiler que desea el usuario, una información acerca del UND del usuario (tal como número de serie de unidad de disco duro, suma de comprobación de BIOS, o otra información que se usa para identificar el UND particular), y una información que identifica al reproductor de medios particular que se usará para acceder al contenido. Entonces, esta información se puede incrustar en la licencia para asegurar que la película solicitada que está asociada con la licencia se reproduce solo en el UND identificado y solo por el reproductor de medios identificado. Una DRM comprueba la GUID de la película que se va a reproducir frente a las GUID de licencias en una Base de Datos Protegida (PD, *Protected Database*). Entonces, la DRM compara el UND y la información de identificación del reproductor de medios en el objeto de datos de licencia identificados con el UND y el reproductor de medios. Si la comprobación es correcta, entonces la DRM comprueba adicionalmente que este es conforme al modelo de alquiler. Si todas las compariciones son verdaderas y si el visionado de la película es conforme al modo de alquiler y, adicionalmente, si las comprobaciones de integridad que son realizadas por la DRM no detectan manipulación indebida alguna, entonces se habilitará la licencia.

El objeto de la presente invención es la provisión de un procedimiento mejorado para proporcionar acceso a un contenido protegido, así como un sistema correspondiente.

Este objeto es solucionado por la materia objeto de las reivindicaciones independientes.

Algunas realizaciones preferidas se definen mediante las reivindicaciones dependientes.

La presente invención se extiende a procedimientos, sistemas y productos de programa informático para la concesión de licencias de contenido protegido para conjuntos de aplicaciones. En algunas realizaciones, un sistema informático detecta que un usuario está intentado acceder a un contenido protegido a través de una aplicación en el sistema informático. El contenido se protege de acuerdo con una directiva de protección que es gestionada por un sistema de gestión de derechos digitales ("DRM", *Digital Rights Management*) que incluye un servidor de gestión de derechos digitales separado. La directiva de protección incluye un conjunto de aplicaciones que identifica un conjunto de aplicaciones a las que se permite acceder al contenido.

Antes de permitir que la aplicación acceda al contenido protegido, el sistema informático intercambia información con el servidor de DRM para obtener una clave de usuario que se corresponde con el usuario. La clave de usuario es para su uso en el acceso al contenido protegido. Asimismo, antes de permitir que la aplicación acceda al contenido protegido, el sistema informático determina que la aplicación se encuentra en el conjunto de aplicaciones. El sistema informático permite que la aplicación use la clave de usuario para acceder al contenido protegido en respuesta a la determinación.

En otras realizaciones, un sistema informático detecta que un usuario está intentado acceder a un contenido protegido a través de una aplicación en el sistema informático. El contenido protegido se protege de acuerdo con una directiva de protección que es especificada por un propietario comercial de una empresa que dio origen al contenido protegido. La directiva de protección indica: usuarios que están autorizados a acceder al contenido, operaciones que a los usuarios autorizados se les permite realizar con respecto al contenido, entornos informáticos a los que se permite acceder al contenido, y un conjunto de aplicaciones a las que se permite acceder al contenido.

El sistema informático envía una información de identidad de usuario para el usuario a un servidor de protección de contenidos. El sistema informático envía el entorno informático del sistema informático al servidor de protección de contenidos. El sistema informático recibe una clave de usuario del servidor de protección. La clave de usuario es utilizable por el usuario para acceder al contenido protegido. La clave de usuario se devuelve del servidor de protección de contenidos al sistema informático en respuesta a autenticar al usuario y en respuesta a determinar que el entorno informático es apropiado para evaluar la pertenencia al conjunto de aplicaciones.

El sistema operativo en el sistema informático determina si la aplicación está incluida en el conjunto de aplicaciones en la directiva de protección. El sistema operativo regula de forma apropiada el acceso de la aplicación al contenido protegido basándose en la determinación. La regulación del sistema operativo puede incluir permitir que la aplicación acceda al contenido protegido cuando la aplicación está incluida en el conjunto de aplicaciones en la directiva de protección. La regulación del sistema operativo también puede incluir evitar que la aplicación acceda al contenido protegido cuando la aplicación no está incluida en el conjunto de aplicaciones en la directiva de protección.

El presente Sumario se proporciona para presentar, en una forma simplificada, una selección de conceptos, que se describen adicionalmente en lo sucesivo en la Descripción detallada. El presente Sumario no tiene por objeto identificar características clave o características esenciales de la materia objeto que se reivindica, ni tiene por objeto su uso como una ayuda en la determinación del alcance de la materia objeto que se reivindica.

Características y ventajas adicionales de la invención se expondrán en la descripción que se da en lo sucesivo, y en parte serán obvias a partir de la descripción, o se pueden aprender mediante la puesta en práctica de la invención. Las características y ventajas de la invención se pueden realizar y obtener por medio de los instrumentos y combinaciones particularmente señalados en las reivindicaciones adjuntas. Estas y otras características de la presente invención serán más plenamente evidentes a partir de la siguiente descripción y las reivindicaciones adjuntas, o se pueden aprender mediante la puesta en práctica de la invención tal como se ha expuesto en lo que antecede en el presente documento.

Breve descripción de los dibujos

Con el fin de describir la forma en la que se pueden obtener las ventajas y características que se han enunciado en lo que antecede de la invención, así como otras ventajas y características, se realizará una descripción más particular de la invención que se ha descrito brevemente en lo que antecede por referencia a algunas realizaciones específicas de la misma que se ilustran en los dibujos adjuntos. Entendiendo que estos dibujos muestran solo algunas realizaciones típicas de la invención y, por lo tanto, no se ha de considerar que sean limitantes de su alcance, la invención se describirá y se explicará con particularidad y detalle adicional a través del uso de los dibujos adjuntos, en los que:

La figura 1 ilustra una vista de una arquitectura informática a modo de ejemplo que facilita la concesión de licencias de contenido protegido para conjuntos de aplicaciones.

La figura 2 ilustra una vista de otra arquitectura informática a modo de ejemplo que facilita la concesión de licencias de contenido protegido para conjuntos de aplicaciones.

La figura 3 ilustra un diagrama de flujo de un procedimiento a modo de ejemplo para proporcionar acceso a un contenido protegido.

La figura 4 ilustra un diagrama de flujo de un procedimiento a modo de ejemplo para proporcionar acceso a un contenido protegido.

Descripción detallada

La presente invención se extiende a procedimientos, sistemas y productos de programa informático para la concesión de licencias de contenido protegido para conjuntos de aplicaciones. En algunas realizaciones, un sistema informático detecta que un usuario está intentado acceder a un contenido protegido a través de una aplicación en el sistema informático. El contenido se protege de acuerdo con una directiva de protección que es gestionada por un sistema de gestión de derechos digitales ("DRM", *Digital Rights Management*) que incluye un servidor de gestión de derechos digitales separado. La directiva de protección incluye un conjunto de aplicaciones que identifica un conjunto de aplicaciones a las que se permite acceder al contenido.

Antes de permitir que la aplicación acceda al contenido protegido, el sistema informático intercambia información con el servidor de DRM para obtener una clave de usuario que se corresponde con el usuario. La clave de usuario es para su uso en el acceso al contenido protegido. Asimismo, antes de permitir que la aplicación acceda al contenido protegido, el sistema informático determina que la aplicación se encuentra en el conjunto de aplicaciones. El sistema informático permite que la aplicación use la clave de usuario para acceder al contenido protegido en respuesta a la determinación.

En otras realizaciones, un sistema informático detecta que un usuario está intentado acceder a un contenido protegido a través de una aplicación en el sistema informático. El contenido protegido se protege de acuerdo con una directiva de protección que es especificada por un propietario comercial de una empresa que dio origen al contenido protegido. La directiva de protección indica: usuarios que están autorizados a acceder al contenido, operaciones que a los usuarios autorizados se les permite realizar con respecto al contenido, entornos informáticos a los que se permite acceder al contenido, y un conjunto de aplicaciones a las que se permite acceder al contenido.

El sistema informático envía una información de identidad de usuario para el usuario a un servidor de protección de contenidos. El sistema informático envía el entorno informático del sistema informático al servidor de protección de contenidos. El sistema informático recibe una clave de usuario del servidor de protección. La clave de usuario es utilizable por el usuario para acceder al contenido protegido. La clave de usuario se devuelve del servidor de protección de contenidos al sistema informático en respuesta a autenticar al usuario y en respuesta a determinar que el entorno informático es apropiado para evaluar la pertenencia al conjunto de aplicaciones.

El sistema operativo en el sistema informático determina si la aplicación está incluida en el conjunto de aplicaciones en la directiva de protección. El sistema operativo regula de forma apropiada el acceso de la aplicación al contenido protegido basándose en la determinación. La regulación del sistema operativo puede incluir permitir que la aplicación acceda al contenido protegido cuando la aplicación está incluida en el conjunto de aplicaciones en la directiva de protección. La regulación del sistema operativo también puede incluir evitar que la aplicación acceda al contenido protegido cuando la aplicación no está incluida en el conjunto de aplicaciones en la directiva de protección.

Algunas realizaciones de la presente invención pueden comprender o utilizar un ordenador de propósito especial o de propósito general que incluye un hardware informático, tal como se analiza con mayor detalle en lo sucesivo. Algunas realizaciones dentro del alcance de la presente invención también incluyen medios legibles por ordenador físicos, y de otro tipo, para portar o almacenar estructuras de datos y / o instrucciones ejecutables por ordenador. Tales medios legibles por ordenador pueden ser cualquier medio disponible al que pueda acceder un sistema informático de propósito general o de propósito especial. Los medios legibles por ordenador que almacenan instrucciones ejecutables por ordenador son medios de almacenamiento físico. Los medios legibles por ordenador que portan instrucciones ejecutables por ordenador son medios de transmisión. Por lo tanto, a modo de ejemplo, y no de limitación, algunas realizaciones de la invención pueden comprender al menos dos tipos claramente diferentes de medios legibles por ordenador: medios de almacenamiento físico y medios de transmisión.

Los medios de almacenamiento físico incluyen RAM, ROM, EEPROM, CD-ROM u otro almacenamiento de disco óptico, almacenamiento de disco magnético, u otros dispositivos de almacenamiento magnético, o cualquier otro medio que se pueda usar para almacenar medios de código de programa deseados en forma de instrucciones ejecutables por ordenador o estructuras de datos y al que pueda acceder un ordenador de propósito general o de propósito especial.

Con esta descripción y las siguientes reivindicaciones, una "red" se define como uno o más enlaces de datos que posibilitan el transporte de datos electrónicos entre módulos y / o sistemas informáticos y / u otros dispositivos electrónicos. Cuando se transfiere o se proporciona una información a través de una red u otra conexión de comunicación (o bien por cable, o bien inalámbrica, o bien una combinación de por cable o inalámbrica) a un ordenador, el ordenador contempla apropiadamente la conexión como un medio de transmisión. Los medios de

transición pueden incluir una red y / o unos enlaces de datos que se pueden usar para portar unos medios de código de programa deseados en forma de instrucciones ejecutables por ordenador o estructuras de datos y a los que pueda acceder un ordenador de propósito general o de propósito especial. Dentro del alcance de los medios legibles por ordenador se deberían incluir, asimismo, combinaciones de lo anterior.

Además, se debería entender que, tras alcanzar diversos componentes de sistema informático, los medios de código de programa en forma de instrucciones ejecutables por ordenador o estructuras de datos se pueden transferir de forma automática de los medios de transmisión a los medios de almacenamiento físico (o viceversa). Por ejemplo, las instrucciones ejecutables por ordenador o estructuras de datos que se reciben a través de una red o enlace de datos se pueden almacenar en memoria intermedia en una RAM dentro de un módulo de interfaz de red (por ejemplo, una "NIC") y, entonces, transferirse con el tiempo a la RAM del sistema informático y / o a unos medios de almacenamiento físico menos volátiles en un sistema informático. Por lo tanto, se ha de entender que se pueden incluir medios de almacenamiento físico en componentes de sistema informático que también (o incluso fundamentalmente) utilizan medios de transmisión.

Las instrucciones ejecutables por ordenador comprenden, por ejemplo, instrucciones que dan lugar a que un ordenador de propósito general, un ordenador de propósito especial u otro dispositivo de procesamiento de propósito especial realice una determinada función o grupo de funciones. Las instrucciones ejecutables por ordenador pueden ser, por ejemplo, códigos binarios, instrucciones en formato intermedio tales como lenguaje de ensamblador, o incluso código fuente. A pesar de que la materia objeto se ha descrito en un lenguaje específico de características estructurales y / o actos metodológicos, se ha de entender que la materia objeto que se define en las reivindicaciones adjuntas no está limitada necesariamente a las características o actos descritos que se han descrito en lo que antecede. Más bien, las características y actos descritos se divulgan como formas a modo de ejemplo de implementación de las reivindicaciones.

Los expertos en la materia apreciarán que la invención se puede poner en práctica en entornos informáticos de red con muchos tipos de configuraciones de sistema informático, incluyendo ordenadores personales, ordenadores de escritorio, ordenadores portátiles, procesadores de mensajes, dispositivos de mano, sistemas de multiprocesador, electrónica de consumo programable o basada en microprocesador, PC de red, miniordenadores, macroordenadores, teléfonos móviles, PDA, buscadores, encaminadores, conmutadores, y similares. La invención también se puede poner en práctica en entornos de sistema distribuidos en los que realizan tareas sistemas informáticos tanto locales como remotos que están enlazados (o bien por enlaces de datos por cable, o enlaces de datos inalámbricos, o bien por una combinación de enlaces de datos por cable e inalámbrico) a través una red. En un entorno de sistema distribuido, los módulos de programa pueden estar ubicados en dispositivos de almacenamiento en memoria tanto locales como remotos.

La figura 1 ilustra una arquitectura informática 100 a modo de ejemplo que facilita la concesión de licencias de contenido protegido para conjuntos de aplicaciones. Tal como se muestra, la arquitectura informática 100 incluye una diversidad de componentes y datos que incluyen el sistema informático 101, el sistema de DRM 171, el servidor de DRM 105, la ubicación de contenidos 104 y la directiva de protección 121. Cada uno de los componentes y datos ilustrados se pueden conectar entre sí a través de un bus de sistema y / o a través de (o ser parte de) una red, tal como, por ejemplo, una Red de Área Local ("LAN", *Local Area Network*), una Red de Área Extensa ("WAN", *Wide Area Network*), e incluso Internet. Por consiguiente, cada uno de los componentes mostrados así como cualquier otro componente conectado, puede crear datos relacionados con mensajes e intercambiar datos relacionados con mensajes (por ejemplo, datagramas de Protocolo de Internet ("IP", *Internet Protocol*) y otros protocolos de capa superior que utilizan datagramas de IP, tales como, el Protocolo de Control de Transmisión ("TCP", *Transmission Control Protocol*), el Protocolo de Transferencia de Hipertexto ("HTTP", *Hypertext Transfer Protocol*), el Protocolo de Transferencia Simple de Correo ("SMTP", *Simple Mail Transfer Protocol*), etc.) a través de la red.

En general, el sistema informático 101 incluye una o más aplicaciones que pueden, de vez en cuando, solicitar acceso a un contenido que está protegido de acuerdo con una directiva de protección. El contenido se puede almacenar en unidades de red remotas, en sitios Web, en bases de datos, en la memoria del sistema informático 101, en servidores de mensajes, etc. El sistema de DRM 171 incluye el servidor de DRM 105. El servidor de DRM 105 puede gestionar directivas de protección para un contenido protegido y dotar a sistemas informáticos de cliente de claves, licencias, etc. para acceder a un contenido protegido.

La figura 3 ilustra un diagrama de flujo de un procedimiento a modo de ejemplo 300 para proporcionar acceso a un contenido protegido. El procedimiento 300 se describirá con respecto a los componentes y datos de la arquitectura informática 100 que se muestra en la figura 1.

El usuario 131 puede introducir la entrada de usuario 111 en la aplicación 103 para solicitar acceso al contenido 113. En respuesta a la entrada de usuario 111, la aplicación 103 puede enviar la solicitud de contenido 112 para intentar acceder al contenido 113 desde la ubicación de contenidos 104. La ubicación de contenidos 104 puede ser virtualmente cualquier ubicación interna (por ejemplo, una memoria de sistema, etc.), local (una unidad de disco duro conectada, etc.) o remota (una unidad de red, un sitio Web, etc.) desde la perspectiva del sistema informático 101.

El procedimiento 300 incluye un acto de detectar que un usuario está intentado acceder a un contenido protegido a través de una aplicación en el sistema informático, protegido el contenido de acuerdo con una directiva de protección que es gestionada por un sistema de gestión de derechos digitales que incluye un servidor de gestión de derechos digitales separado, incluyendo la directiva de protección un conjunto de aplicaciones, identificando el conjunto de aplicaciones un conjunto de aplicaciones a las que se permite acceder al contenido (el acto 301). Por ejemplo, el sistema informático 101 puede detectar que la solicitud de contenido 112 es un intento de acceder al contenido 113 desde la ubicación de contenidos 104. El contenido 113 se puede proteger de acuerdo con la directiva de protección 121 que es gestionada por el servidor de DRM 105. La directiva de protección 121 incluye el conjunto de aplicaciones 124 que identifica un conjunto de aplicaciones a las que se permite el acceso al contenido.

Las aplicaciones se pueden identificar mediante una ID de aplicación. Una ID de aplicación se puede basar en una o más de una aplicación, una versión de la aplicación, un historial de revisiones de la aplicación, una propiedad de la aplicación, una certificación de la aplicación, etc. Por lo tanto, el conjunto de aplicaciones 124 puede incluir una lista de ID de aplicación.

Antes de permitir que la aplicación acceda al contenido protegido, el procedimiento 300, un acto de intercambiar, el sistema informático, una información con el servidor de gestión de derechos digitales para obtener una clave de usuario que se corresponde con el usuario, la clave de usuario para acceder al contenido protegido (el acto 302). Por ejemplo, el sistema informático 101 y el servidor de DRM 105 pueden realizar un intercambio de autenticación 114 que da como resultado la emisión de la clave de usuario 117 (que se corresponde con el usuario 131) al sistema informático 101.

Antes de permitir que la aplicación acceda al contenido protegido, el procedimiento 300 también puede incluir un acto de determinar, el sistema informático, que la aplicación se encuentra en el conjunto de aplicaciones (el acto 303). Por ejemplo, el sistema informático 101 puede determinar que la aplicación 103 está incluida en el conjunto de aplicaciones 124. El sistema informático 101 puede generar o acceder a una ID de aplicación previamente generada para la aplicación 103. La ID de aplicación se puede generar a partir de una o más de la aplicación, la versión de la aplicación, el historial de revisiones de la aplicación, la propiedad de la aplicación, la certificación de la aplicación, etc. de la aplicación 103. El sistema informático 101 puede comparar la ID de aplicación para la aplicación 103 con las ID de aplicación que están incluidas en el conjunto de aplicaciones 124. En respuesta a que la comparación revele que la ID de aplicación para la aplicación 103 está incluida en el conjunto de aplicaciones 124, el sistema informático 101 determina que la aplicación 103 está incluida en el conjunto de aplicaciones 124.

El procedimiento 300 incluye un acto de permitir, el sistema informático, que la aplicación use la clave de usuario para acceder al contenido protegido en respuesta a la determinación (el acto 304). Por ejemplo, el sistema informático 101 puede permitir que la aplicación 103 use la clave de usuario 117 para acceder al contenido 113 (desde la ubicación de contenidos 104) en respuesta a determinar que la aplicación 103 está incluida en el conjunto de aplicaciones 124.

En algunas realizaciones, también se considera un entorno operativo cuando se determina si se ha de permitir o denegar el acceso a un contenido protegido. La figura 2 ilustra una arquitectura informática 200 a modo de ejemplo que facilita la concesión de licencias de contenido protegido para conjuntos de aplicaciones. Tal como se muestra, la arquitectura informática 200 incluye una diversidad de componentes y datos que incluyen el sistema informático 201, el servidor de protección 105, la ubicación de contenidos 204 y la directiva de protección 221. Cada uno de los componentes y datos ilustrados se pueden conectar entre sí a través de un bus de sistema y / o a través de (o ser parte de) una red, tal como, por ejemplo, una Red de Área Local ("LAN", *Local Area Network*), una Red de Área Extensa ("WAN", *Wide Area Network*), e incluso Internet. Por consiguiente, cada uno de los componentes mostrados así como cualquier otro componente conectado, puede crear datos relacionados con mensajes e intercambiar datos relacionados con mensajes (por ejemplo, datagramas de Protocolo de Internet ("IP", *Internet Protocol*) y otros protocolos de capa superior que utilizan datagramas de IP, tales como, el Protocolo de Control de Transmisión ("TCP", *Transmission Control Protocol*), el Protocolo de Transferencia de Hipertexto ("HTTP", *Hypertext Transfer Protocol*), el Protocolo de Transferencia Simple de Correo ("SMTP", *Simple Mail Transfer Protocol*), etc.) a través de la red.

En general, el sistema informático 202 incluye una o más aplicaciones 203A, 203B, etc. que se ejecutan dentro del sistema operativo 202. Las una o más aplicaciones pueden, de vez en cuando, solicitar acceso a un contenido que está protegido de acuerdo con una directiva de protección. El contenido se puede almacenar en unidades de red remotas, en sitios Web, en bases de datos, en la memoria del sistema informático 201, en servidores de mensajes, etc. El servidor de protección 205 puede gestionar directivas de protección para un contenido protegido y dotar a sistemas informáticos de cliente de claves, licencias, etc. para acceder a un contenido protegido.

La figura 4 ilustra un diagrama de flujo de un procedimiento a modo de ejemplo 400 para proporcionar acceso a un contenido protegido. El procedimiento 400 se describirá con respecto a los componentes y datos de la arquitectura informática 200 que se muestra en la figura 2.

El usuario 331 puede introducir la entrada de usuario 211 en la aplicación 203B para solicitar acceso al contenido protegido 213. En respuesta a la entrada de usuario 211, la aplicación 203B puede enviar la solicitud de contenido

212 para intentar acceder al contenido protegido 213 desde la ubicación de contenidos 204. La ubicación de contenidos 204 puede ser virtualmente cualquier ubicación interna (por ejemplo, una memoria de sistema, etc.), local (una unidad de disco duro conectada, etc.) o remota (una unidad de red, un sitio Web, etc.) desde la perspectiva del sistema informático 101.

El procedimiento 400 incluye un acto de detectar que un usuario está intentado acceder a un contenido protegido a través de una aplicación en el sistema informático, protegido el contenido protegido de acuerdo con una directiva de protección, especificada la directiva de protección por un propietario comercial de una empresa que dio origen al contenido protegido, indicando la directiva de protección: usuarios que están autorizados a acceder al contenido, operaciones que a los usuarios autorizados se les permite realizar con respecto al contenido, entornos informáticos a los que se permite acceder al contenido, y un conjunto de aplicaciones a las que se permite acceder al contenido (el acto 401). Por ejemplo, el sistema operativo 202 puede detectar que la solicitud de contenido 212 es un intento de acceder al contenido protegido 213 desde la ubicación de contenidos 204. El contenido protegido 213 se puede proteger de acuerdo con la directiva de protección 221 que es gestionada por el servidor de protección 205. La directiva de protección 221 puede ser especificada por el propietario comercial que dio origen al contenido protegido 213.

La directiva de protección 221 incluye los permisos de usuario 222, los entornos autorizados 223 y las aplicaciones autorizadas 224. Los permisos de usuario 222 representan una combinación de usuarios autorizados para el contenido protegido 213 y operaciones que a los usuarios autorizados del contenido protegido 213 se les permite realizar con respecto al contenido protegido 213. De forma similar al conjunto de aplicaciones 124, las aplicaciones autorizadas 224 pueden indicar (por ejemplo, mediante una ID de aplicación) aplicaciones que están autorizadas a acceder al contenido protegido 213. Las aplicaciones autorizadas 224 también pueden representar aplicaciones en las que se confía para regular de forma apropiada el acceso al contenido protegido 213 de acuerdo con los permisos de uso 222.

Un entorno operativo puede incluir una combinación de uno o más atributos de sistema incluyendo: una ubicación de red (física o lógica), una ruta de arranque, una directiva de integridad de código, opciones de arranque (por ejemplo, depurador de modo de núcleo habilitado, modo seguro, etc.), información procedente de un agente de salud de sistema ("SHA", *system health agent*), información procedente de un validador de salud de sistema ("SHV", *system health validator*), etc. Los entornos autorizados 223 indican unos entornos operativos en los que confía el servidor de protección 205 para realizar la evaluación del conjunto de aplicaciones. Diferentes combinaciones de atributos de sistema pueden dar como resultado diferentes entornos operativos autorizados.

El procedimiento 300 incluye un acto de enviar una información de identidad de usuario para el usuario a un servidor de protección de contenidos (el acto 402). Por ejemplo, el sistema informático 101 puede enviar una información de identidad 215, tal como, por ejemplo, credenciales de usuario, al servidor de protección 205. El procedimiento 400 incluye un acto de enviar el entorno informático del sistema informático al servidor de protección de contenidos (el acto 403). Por ejemplo, el sistema informático 101 puede enviar el entorno informático 216 al servidor de protección 205.

El entorno informático 216 puede incluir una combinación de atributos de sistema del sistema informático 201. El sistema informático 201 puede usar atestación, o algún otro mecanismo seguro, para enviar el entorno informático al servidor de protección 205 de una forma en la que confía el servidor de protección 205. El entorno informático 216 puede incluir una o más de: una ubicación de red (física o lógica) para el sistema informático 201, una ruta de arranque del sistema operativo 202, una directiva de integridad de código del sistema operativo 202, opciones de arranque del sistema operativo 202 (por ejemplo, depurador de modo de núcleo habilitado, modo seguro, etc.), información procedente de un agente de salud de sistema ("SHA", *system health agent*) en ejecución en el sistema informático 201, información procedente de un validador de salud de sistema ("SHV", *system health validator*) en ejecución en el sistema informático 201, etc.

El servidor de protección 205 puede usar la información de identidad 214 para determinar si el usuario 231 es un usuario autorizado del contenido protegido 213. Por ejemplo, el servidor de protección 205 puede usar la información de identidad 214 para localizar permisos para el usuario 231 en los permisos de usuario 222.

El servidor de protección 205 puede usar el entorno informático 216 para determinar si el sistema informático 201 tiene un entorno informático apropiado para evaluar la pertenencia al conjunto de aplicaciones. Un entorno apropiado para evaluar la pertenencia al conjunto de aplicaciones puede indicar que el servidor de protección 205 está dispuesto a confiar en el entorno informático para evaluar de forma apropiada la pertenencia al conjunto de aplicaciones. Por ejemplo, el servidor de protección 205 puede analizar los atributos de sistema en el entorno informático 216 para determinar si alguna combinación de atributos de sistema que están incluidos en el entorno informático 216 son indicativos de un entorno informático que está incluido en los entornos autorizados 223 (y, por lo tanto, se puede confiar en el mismo para realizar la evaluación del conjunto de aplicaciones).

Diferentes atributos de sistema individuales o combinaciones de atributos de sistema pueden indicar un entorno informático autorizado. Por ejemplo, una dirección de red indicativa de un sistema informático en una red local podría ser evidencia suficiente de un entorno apropiado para evaluar la pertenencia al conjunto de aplicaciones. Por

otro lado, para un sistema informático fuera de un cortafuegos, se puede requerir una ruta de arranque bien conocida, una directiva de integridad de código suficiente y una información de salud especificada como evidencia para indicar un entorno apropiado para evaluar la pertenencia al conjunto de aplicaciones.

Cuando el usuario 231 es un usuario autorizado del contenido protegido 213 y el entorno informático 216 es un entorno informático autorizado, el servidor de protección 205 puede devolver la clave de usuario 217 al sistema informático 201.

El procedimiento 400 incluye un acto de recibir una clave de usuario del servidor de protección, utilizable la clave de usuario por el usuario para acceder al contenido protegido, devuelta la clave de usuario del servidor al sistema informático en respuesta a autenticar al usuario y en respuesta a determinar que el entorno informático es apropiado para evaluar la pertenencia al conjunto de aplicaciones (el acto 404). Por ejemplo, el sistema informático 201 puede recibir la clave de usuario 217 del servidor de protección 205. La clave de usuario 217 es utilizable por el usuario 231 para acceder al contenido protegido 213. La clave de usuario 217 se devuelve al sistema informático 201 en respuesta a que el servidor de protección 205 autentique al usuario 231 y a que determine que el entorno operativo del sistema informático 101 es apropiado para evaluar la pertenencia al conjunto de aplicaciones para la aplicación 203B.

El procedimiento 400 incluye un acto de determinar, un sistema operativo en el sistema informático, si la aplicación está incluida en el conjunto de aplicaciones en la directiva de protección (el acto 405). Por ejemplo, el sistema operativo 202 puede determinar si la aplicación 203 está incluida en las aplicaciones autorizadas 224. El sistema operativo 202 puede comparar una ID de aplicación para la aplicación 203 con las ID de aplicación que están incluidas en las aplicaciones autorizadas 224. Si la comparación revela una coincidencia, el sistema operativo 202 determina que la aplicación 203B es una aplicación autorizada. Si la comparación no revela una coincidencia, el sistema operativo 202 determina que la aplicación 203B no es una aplicación autorizada.

El procedimiento 400 incluye un acto de regular de forma apropiada, el sistema operativo, el acceso de la aplicación al contenido protegido basándose en la determinación (el acto 406). Por ejemplo, el sistema operativo 202 puede regular de forma apropiada el acceso de la aplicación 203B al contenido protegido 213 basándose en si la aplicación 203B es una aplicación autorizada o la aplicación 203B no es una aplicación autorizada.

Por lo tanto, una regulación apropiada del acceso de aplicaciones a un contenido protegido puede incluir un acto de permitir, el sistema operativo, que la aplicación acceda al contenido protegido cuando la aplicación está incluida en el conjunto de aplicaciones en la directiva de protección (el acto 407). Por ejemplo, cuando la aplicación 203B está incluida en las aplicaciones autorizadas 224, el sistema operativo 202 puede permitir que la aplicación 203B use la clave de usuario 217 para acceder al contenido protegido 213. Por consiguiente, la aplicación 203B puede imponer los permisos de usuario 222 para el usuario 231 con respecto al contenido protegido 213.

Por otro lado, una regulación apropiada del acceso de aplicaciones a un contenido protegido también puede incluir un acto de impedir, el sistema operativo, que la aplicación acceda al contenido protegido cuando la aplicación no está incluida en el conjunto de aplicaciones en la directiva de protección (el acto 408). Por ejemplo, cuando la aplicación 203B no está incluida en las aplicaciones autorizadas 224, el sistema operativo 202 puede evitar que la aplicación 203B acceda al contenido protegido 213. La carencia de autorización puede indicar que no se confía en la aplicación 203B para imponer los permisos de usuario 222 para el contenido protegido 213.

Por consiguiente, algunas realizaciones de la invención permiten a una máquina local una participación aumentada en la autorización de acceso a un contenido protegido. Por ejemplo, se permite a un sistema operativo dentro de un entorno informático apropiado determinar si una aplicación está autorizada a acceder al contenido protegido. Por lo tanto, se libera a la aplicación de tener que almacenar una licencia de publicación. Además, las decisiones de autorización están parcialmente distribuidas, lo que alivia la carga de recursos en un servidor de protección. Por consiguiente, algunas realizaciones de la invención pueden facilitar unas decisiones de autorización más robustas y eficientes cuando se solicita acceso a un contenido protegido. Las realizaciones descritas se han de considerar solo como ilustrativas y no como restrictivas. El alcance de la invención se define mediante las reivindicaciones adjuntas.

REIVINDICACIONES

1. En un sistema informático (101), un procedimiento para proporcionar acceso a un contenido protegido (113), comprendiendo el procedimiento:

un acto de detectar, por el sistema informático, que un usuario (131) está intentando acceder a un contenido protegido a través de una aplicación (103) en el sistema informático (112), protegido el contenido protegido de acuerdo con una directiva de protección (121) que es gestionada por un sistema de gestión de derechos digitales, DRM, (171) que incluye un servidor de gestión de derechos digitales (105) separado, incluyendo la directiva de protección (121) un conjunto de aplicaciones (124) y uno o más entornos informáticos, identificando el conjunto de aplicaciones (124) un conjunto de aplicaciones a las que se permite acceder al contenido;
antes de permitir que la aplicación (103) acceda al contenido protegido (113):

un acto de intercambiar, por el sistema informático, una información (114) con el servidor de gestión de derechos digitales (105), incluyendo la información uno o más atributos del entorno operativo del sistema informático y una información de autenticación de usuario para el usuario, usados los uno o más atributos por el servidor de DRM para determinar que se confía en el sistema informático para evaluar si la aplicación se encuentra en el conjunto de aplicaciones;
basándose al menos en parte en el intercambio de información del sistema informático con el servidor de DRM (105), un acto de obtener, por el sistema informático, una clave de usuario (117) que se corresponde con el usuario (131), siendo la clave de usuario utilizable para acceder al contenido protegido (113), emitida la clave de usuario por el servidor de DRM después de determinar que el usuario está autorizado a acceder al contenido protegido y después de determinar que se confía en el sistema informático para evaluar si la aplicación se encuentra en el conjunto de aplicaciones; y
un acto de determinar, por el sistema informático (101), que la aplicación (103) se encuentra en el conjunto de aplicaciones (124); y

posteriormente a determinar, por el sistema informático, que la aplicación se encuentra en el conjunto de aplicaciones, un acto de permitir, por el sistema informático (101), que la aplicación (103) use la clave de usuario (117) para acceder al contenido protegido (113).

2. El procedimiento de acuerdo con la reivindicación 1, en el que el acto de detectar que un usuario está intentado acceder a un contenido protegido a través de una aplicación en el sistema informático comprende uno de:

un acto de detectar que un usuario está intentado acceder a un contenido protegido que está protegido de acuerdo con una directiva de protección, incluyendo la directiva de protección un conjunto de aplicaciones, en el que el conjunto de aplicaciones incluye una o más ID de aplicación para aplicaciones que están autorizadas a acceder al contenido protegido; y
un acto de detectar que un usuario está intentando acceder a un contenido protegido, protegido el contenido protegido de acuerdo con una directiva de protección del propietario comercial del contenido protegido.

3. El procedimiento de acuerdo con la reivindicación 1, en el que los atributos del entorno operativo del sistema informático indican una o más de una ubicación de red, una ruta de arranque para el sistema operativo, una directiva de integridad de código para el sistema operativo, opciones de arranque para el sistema operativo, información procedente de un agente de salud de sistema, SHA, e información procedente de un validador de salud de sistema, SHV.

4. El procedimiento de acuerdo con la reivindicación 1, en el que el acto de determinar, por el sistema informático, que la aplicación se encuentra en el conjunto de aplicaciones comprende un acto de determinar, un sistema operativo en el sistema informático, que la aplicación se encuentra en el conjunto de aplicaciones.

5. El procedimiento de acuerdo con la reivindicación 1, en el que el acto de determinar, por el sistema informático, que la aplicación se encuentra en el conjunto de aplicaciones comprende:

un acto de comparar, por el sistema informático, una ID de aplicación de la aplicación con las ID de aplicación que están incluidas en el conjunto de aplicaciones; y
un acto de determinar que la ID de aplicación de la aplicación está incluida en el conjunto de aplicaciones.

6. El procedimiento de la reivindicación 1, en el que la directiva de protección (221) indica adicionalmente usuarios que están autorizados a acceder al contenido (222), operaciones que a los usuarios autorizados se les permite realizar con respecto al contenido protegido, y entornos informáticos a los que se permite acceder al contenido (223), y en el que un sistema operativo (202) en el sistema informático (201) determina si la aplicación (203b) está incluida en el conjunto de aplicaciones (224) en la directiva de protección (221), comprendiendo adicionalmente el procedimiento un acto de regular de forma apropiada, por el sistema operativo (202), el acceso de la aplicación (203B) al contenido protegido (213) basándose en la determinación, incluyendo:

un acto de permitir que la aplicación (203B) acceda al contenido protegido (213) cuando la aplicación (203B) está incluida en el conjunto de aplicaciones (224) en la directiva de protección (221); y

un acto de evitar que la aplicación (203B) acceda al contenido protegido (213) cuando la aplicación (203B) no está incluida en el conjunto de aplicaciones (224) en la directiva de protección (221).

7. El procedimiento de acuerdo con la reivindicación 6, en el que el acto de detectar que un usuario está intentado acceder a un contenido protegido a través de una aplicación en el sistema informático, protegido el contenido protegido de acuerdo con una directiva de protección, comprende uno de:

un acto de detectar que un usuario está intentado acceder a un contenido protegido a través de una aplicación en el sistema informático, protegido el contenido protegido de acuerdo con una directiva de protección, en el que los entornos informáticos a los que se permite acceder al contenido comprenden entornos informáticos en los que se confía lo suficiente para evaluar la pertenencia al conjunto de aplicaciones; y
un acto de detectar que un usuario está intentado acceder a un contenido protegido a través de una aplicación en el sistema informático, protegido el contenido protegido de acuerdo con una directiva de protección, en el que las aplicaciones autorizadas son aplicaciones en las que se confía para imponer de forma apropiada las operaciones que a los usuarios se les permite realizar.

8. El procedimiento de acuerdo con la reivindicación 6, en el que un acto de enviar una información de usuario para el usuario al servidor de DRM comprende un acto de enviar credenciales de usuario al servidor de DRM.

9. El procedimiento de acuerdo con la reivindicación 6, en el que los atributos del entorno operativo del ordenador indican una o más de una ubicación de red, una ruta de arranque para el sistema operativo, una directiva de integridad de código para el sistema operativo, opciones de arranque para el sistema operativo, información procedente de un agente de salud de sistema, SHA, e información procedente de un validador de salud de sistema, SHV.

10. El procedimiento de acuerdo con la reivindicación 6, en el que el acto de determinar, por el sistema operativo, si la aplicación está incluida en el conjunto de aplicaciones en la directiva de protección comprende uno de:

un acto de comparar, por el sistema operativo, una ID de aplicación para la aplicación con las ID de aplicación que están incluidas en la directiva de protección; y
un acto de determinar, por el sistema operativo, que la aplicación está incluida en el conjunto de aplicaciones.

11. El procedimiento de acuerdo con la reivindicación 6, en el que el acto de permitir que la aplicación acceda al contenido protegido comprende un acto de imponer, la aplicación, operaciones que a los usuarios autorizados se les permite realizar con respecto al contenido protegido.

12. Un sistema informático, comprendiendo el sistema informático:

uno o más procesadores;
una memoria de sistema; y
uno o más medios legibles por ordenador que tienen, almacenados en los mismos, unas instrucciones ejecutables por ordenador que, cuando son ejecutadas por uno de los procesadores, dan lugar a que el sistema informático proporcione acceso a un contenido protegido, y que lleve a cabo unas acciones que incluyen lo siguiente:

detectar que un usuario está intentado acceder a un contenido protegido a través de una aplicación (103) en el sistema informático, protegido el contenido protegido de acuerdo con una directiva de protección de gestión de derechos digitales, DRM, (121), especificada la directiva de protección de DRM por un propietario comercial de una empresa que dio origen al contenido protegido, indicando la directiva de protección: usuarios que están autorizados a acceder al contenido, operaciones que a los usuarios autorizados se les permite realizar con respecto al contenido protegido, entornos informáticos a los que se permite acceder al contenido, y un conjunto de aplicaciones (124) a las que se permite acceder al contenido;
enviar credenciales de usuario para el usuario a un servidor de DRM (105);
enviar uno o más atributos de sistema del sistema informático al servidor de DRM para indicar que el servidor de DRM puede confiar en el entorno informático del sistema informático para evaluar si la aplicación en el sistema informático se encuentra en el conjunto de aplicaciones a las que se permite acceder al contenido;
recibir una clave de usuario (117) del servidor de DRM, utilizable la clave de usuario por el usuario para acceder al contenido protegido, devuelta la clave de usuario del servidor de DRM al sistema informático en respuesta a autenticar al usuario con las credenciales y en respuesta a determinar que los uno o más atributos de sistema indican un entorno informático que es apropiado para evaluar si la aplicación se encuentra en el conjunto de aplicaciones a las que se permite acceder al contenido de acuerdo con la directiva de protección;
determinar, un sistema operativo en el sistema informático, si la aplicación está incluida en el conjunto de aplicaciones en la directiva de protección, inclusión en el conjunto de aplicaciones indicativa de una aplicación en la que se confía para imponer operaciones que a los usuarios autorizados se les permite realizar con respecto al contenido protegido; y
regular de forma apropiada, por el sistema operativo, el acceso de la aplicación al contenido protegido basándose en la determinación, incluyendo:

permitir que la aplicación imponga operaciones que a los usuarios autorizados se les permite realizar con respecto al contenido protegido cuando la aplicación está incluida en el conjunto de aplicaciones en la directiva de protección; y

evitar que la aplicación acceda al contenido protegido cuando la aplicación no está incluida en el conjunto de aplicaciones en la directiva de protección.

13. El sistema de acuerdo con la reivindicación 12, en el que las aplicaciones no de confianza que están excluidas de la pertenencia al conjunto son marcadas como no utilizables por el sistema operativo para imponer operaciones que a los usuarios autorizados se les permite realizar con respecto al contenido protegido.

14. El sistema de acuerdo con la reivindicación 12, en el que las instrucciones ejecutables por ordenador, cuando son ejecutadas por uno de los procesadores, dan lugar a que el sistema informático determine si la aplicación está incluida en el conjunto de aplicaciones en la directiva de protección y compare una ID de aplicación para la aplicación con las ID de aplicación en el conjunto de las aplicaciones.

15. El sistema de acuerdo con la reivindicación 12, en el que los atributos de sistema del sistema informático que se envían al servidor de DRM comprenden una o más de: una ubicación de red, una ruta de arranque para el sistema operativo, una directiva de integridad de código para el sistema operativo, opciones de arranque para el sistema operativo, información procedente de un agente de salud de sistema, SHA, e información procedente de un validador de salud de sistema, SHV.

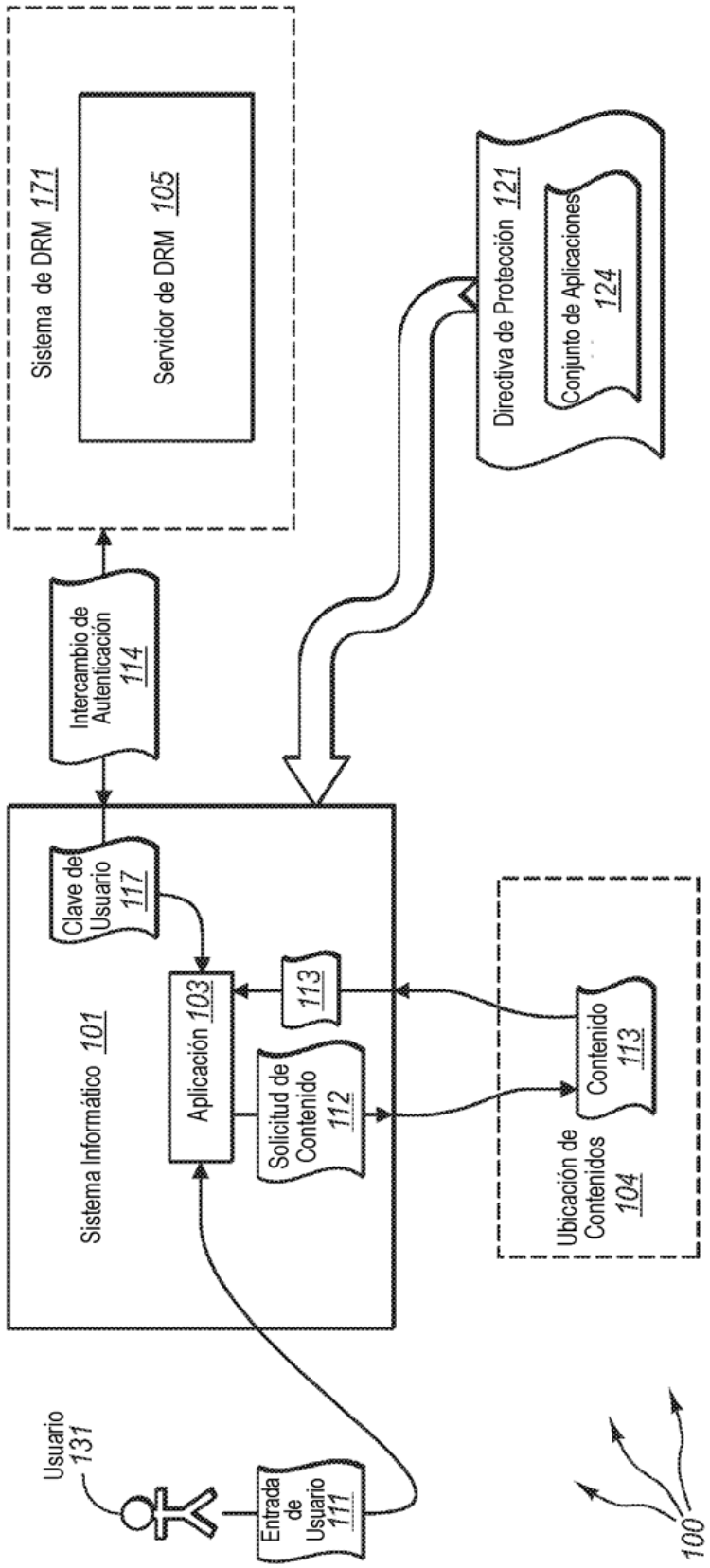
Sistema de DRM 171
Servidor de DRM 105
Directiva de Protección 121
Conjunto de Aplicaciones 124
Intercambio de Autenticación 114
Clave de Usuario 117
Sistema Informático 101
Aplicación 103
113
Solicitud de Contenido 112
Contenido 113
Ubicación de Contenidos 104
Usuario 131
Entrada de Usuario 111
100

FIG. 1

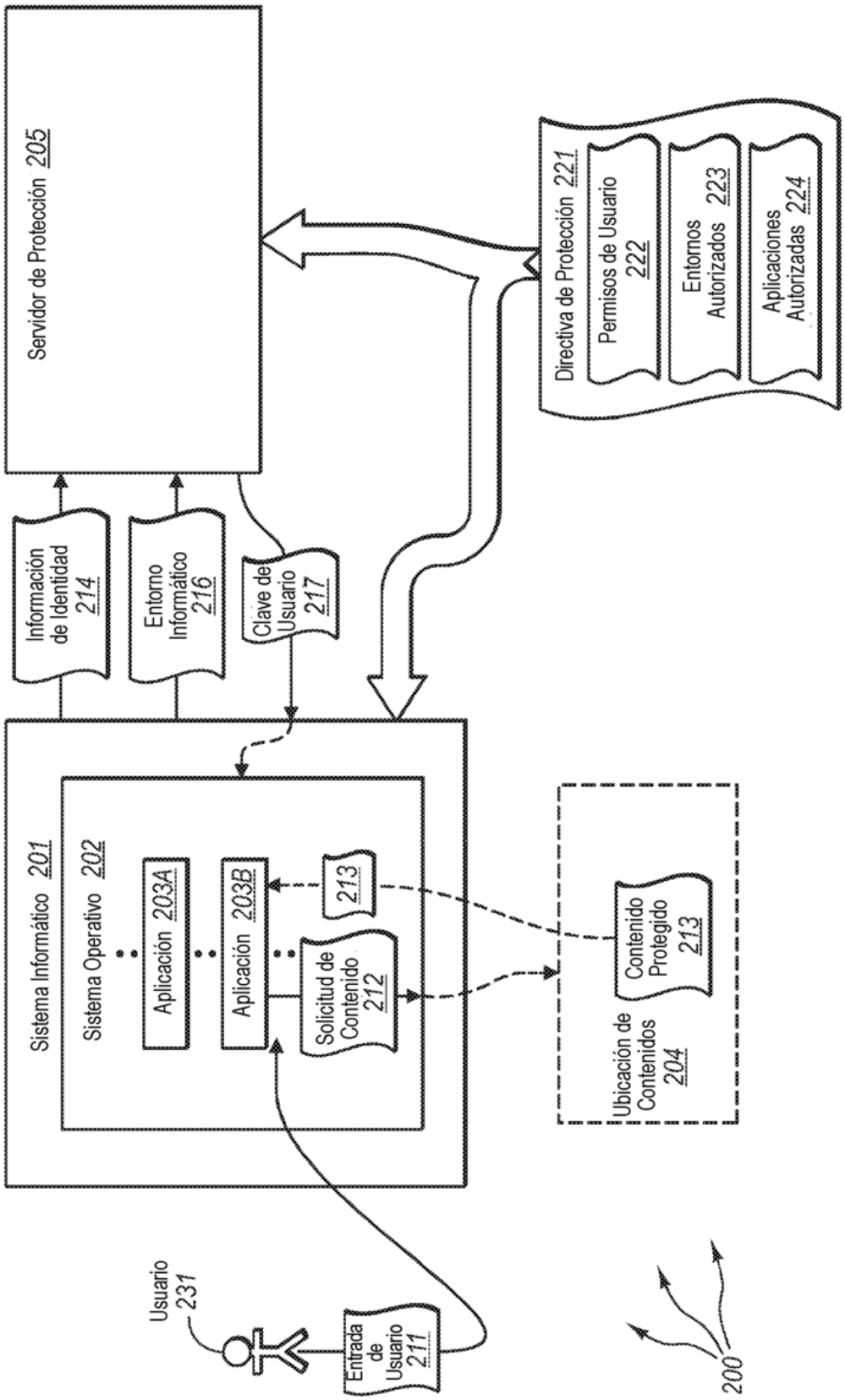
Servidor de Protección 205
Directiva de Protección 221
Permisos de Usuario 222
Entornos Autorizados 223
Aplicaciones Autorizadas 224
Información de Identidad 214
Entorno Informático 216
Clave de Usuario 217
Sistema Informático 201
Sistema Operativo 202
Aplicación 203A
Aplicación 203B
Solicitud de Contenido 212
213
Ubicación de Contenidos 204
Contenido Protegido 213
Usuario 231
Entrada de Usuario 211
200

FIG. 2

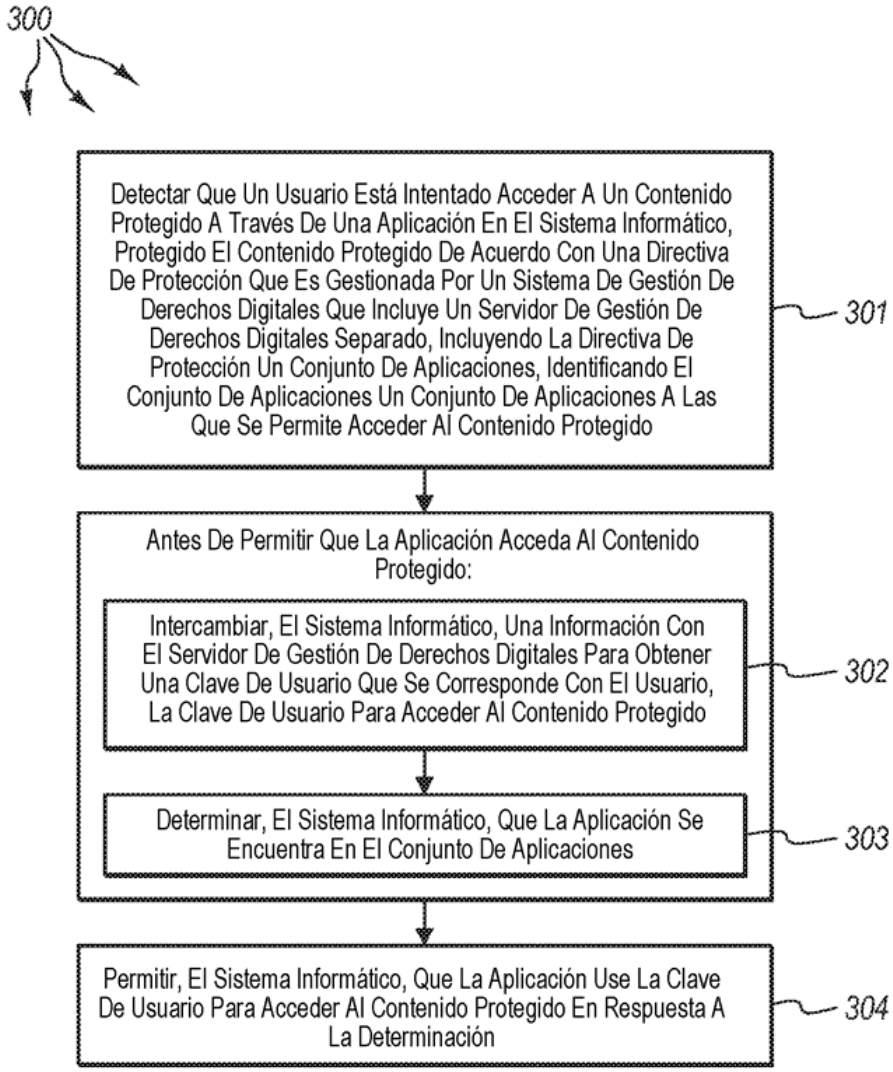
300
Detectar Que Un Usuario Está Intentado Acceder A Un Contenido Protegido A Través De Una Aplicación En El Sistema Informático, Protegido El Contenido Protegido De Acuerdo Con Una Directiva De Protección Que Es Gestionada Por Un Sistema De Gestión De Derechos Digitales Que Incluye Un Servidor De Gestión De Derechos Digitales Separado, Incluyendo La Directiva De Protección Un Conjunto De Aplicaciones, Identificando El Conjunto De Aplicaciones Un Conjunto De Aplicaciones A Las Que Se Permite Acceder Al Contenido Protegido
301
Antes De Permitir Que La Aplicación Acceda Al Contenido Protegido:
Intercambiar, El Sistema Informático, Una Información Con El Servidor De Gestión De Derechos Digitales Para Obtener Una Clave De Usuario Que Se Corresponde Con El Usuario, La Clave De Usuario Para Acceder Al Contenido Protegido
302
Determinar, El Sistema Informático, Que La Aplicación Se Encuentra En El Conjunto De Aplicaciones
303
Permitir, El Sistema Informático, Que La Aplicación Use La Clave De Usuario Para Acceder Al Contenido Protegido En Respuesta A La Determinación
304

FIG. 3

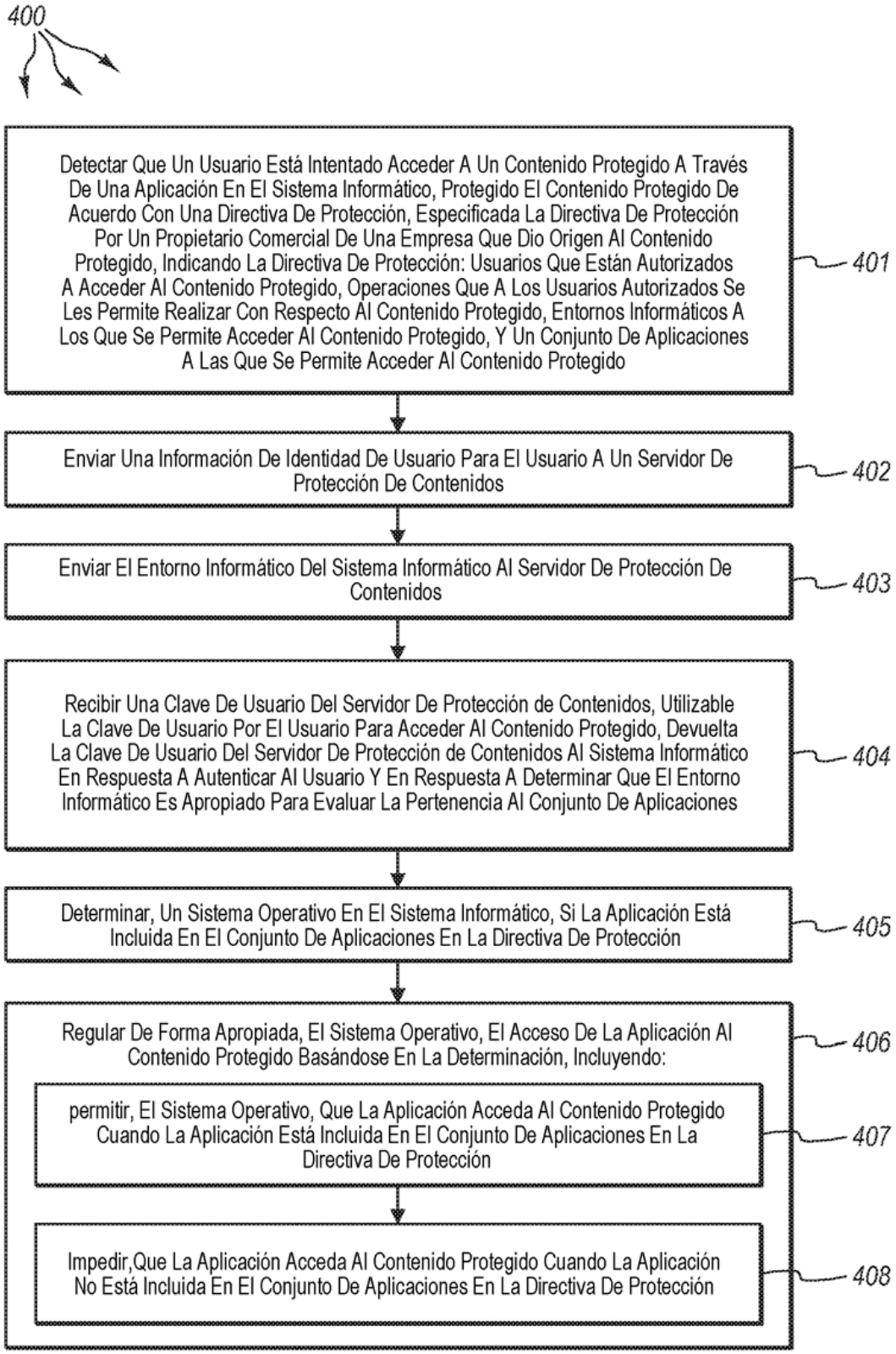
400
Detectar Que Un Usuario Está Intentado Acceder A Un Contenido Protegido A Través De Una Aplicación En El Sistema Informático, Protegido El Contenido Protegido De Acuerdo Con Una Directiva De Protección, Especificada La Directiva De Protección Por Un Propietario Comercial De Una Empresa Que Dio Origen Al Contenido Protegido, Indicando La Directiva De Protección: Usuarios Que Están Autorizados A Acceder Al Contenido Protegido, Operaciones Que A Los Usuarios Autorizados Se Les Permite Realizar Con Respecto Al Contenido Protegido, Entornos Informáticos A Los Que Se Permite Acceder Al Contenido Protegido, Y Un Conjunto De Aplicaciones A Las Que Se Permite Acceder Al Contenido Protegido
401
Enviar Una Información De Identidad De Usuario Para El Usuario A Un Servidor De Protección De Contenidos
402
Enviar El Entorno Informático Del Sistema Informático Al Servidor De Protección De Contenidos
403
Recibir Una Clave De Usuario Del Servidor De Protección de Contenidos, Utilizable La Clave De Usuario Por El Usuario Para Acceder Al Contenido Protegido, Devuelta La Clave De Usuario Del Servidor De Protección de Contenidos Al Sistema Informático En Respuesta A Autenticar Al Usuario Y En Respuesta A Determinar Que El Entorno Informático Es Apropiado Para Evaluar La Pertenencia Al Conjunto De Aplicaciones
404
Determinar, Un Sistema Operativo En El Sistema Informático, Si La Aplicación Está Incluida En El Conjunto De Aplicaciones En La Directiva De Protección
405
Regular De Forma Apropiada, El Sistema Operativo, El Acceso De La Aplicación Al Contenido Protegido Basándose En La Determinación, Incluyendo:
406
permitir, El Sistema Operativo, Que La Aplicación Acceda Al Contenido Protegido Cuando La Aplicación Está Incluida En El Conjunto De Aplicaciones En La Directiva De Protección
407
Impedir,Que La Aplicación Acceda Al Contenido Protegido Cuando La Aplicación No Está Incluida En El Conjunto De Aplicaciones En La Directiva De Protección
408

FIG. 4