(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 555 852**

(51) Int. CI.:

G06F 21/10 (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **17.12.2008 E 08867280 (3)**

(97) Fecha y número de publicación de la concesión europea: **21.10.2015 EP 2225691**

(54) Título: **Dispositivo y procedimiento para la gestión de derechos digitales**

(30) Prioridad:

20.12.2007 CN 200710159812

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
11.01.2016

(73) Titular/es:

KONINKLIJKE PHILIPS N.V. (100.0%)
HIGH TECH CAMPUS 5
5656 AE EINDHOVEN, NL

(72) Inventor/es:

QU, JIN y
MA, FULONG

(74) Agente/Representante:

ISERN JARA, Jorge

DESCRIPCIÓN

Dispositivo y procedimiento para la gestión de derechos digitales

Campo técnico

La presente invención se refiere a la técnica de Gestión de Derechos Digitales (DRM); en particular, a un procedimiento para la protección de derechos digitales en base a técnicas de cifrado y autenticación de validez, y a un dispositivo y a un procedimiento para representar los contenidos digitales que tengan protección de derechos digitales.

Técnica de fondo

Las características de la información digitalizada requieren que haya una única técnica para mejorar la protección del derecho de autor de tales contenidos de programas de audio y vídeo digitalizados, y tal técnica se llama la técnica de Gestión de Derechos Digitales (DRM).

El principio operativo de la técnica de Gestión de Derechos Digitales es habitualmente tal como: se establece primero un centro de autorización de contenido digital, para codificar los contenidos digitales comprimidos, los contenidos digitales son cifrados con una clave, y la cabecera de los contenidos digitales cifrados almacena el Identificador de contenido digital y la dirección del centro de autorización. Cuando el usuario representa (reproduce) los contenidos digitales, una licencia para la clave incrustada relevante de descifrado es enviada al usuario, después de la autenticación y la autorización, por el centro de autorización de contenido digital, de acuerdo al Identificador de contenido y la información de dirección en la cabecera del programa, y luego los contenidos digitales pueden ser representados. Dado que los contenidos a proteger están cifrados y, por tanto, aunque sean descargados y almacenados por un usuario, no pueden ser representados sin la autenticación y la autorización por parte del centro de autorización de programas digitales. En consecuencia, el derecho de autor del programa está estrictamente protegido.

En la técnica anterior, hay tres tipos de modalidad de DRM. Una de ellas es la DRM basada en dispositivos, en la que un derecho para representar un elemento de contenido digital es concedido a uno o a varios dispositivos; otra modalidad es la DRM basada en usuarios, en la que el derecho es concedido a un usuario; y la otra modalidad es la DRM híbrida, en la que el derecho es concedido a un dispositivo o a un usuario, y esto significa que cualquier usuario puede representar el contenido digital cifrado en el dispositivo autorizado, y el usuario autorizado puede representar el contenido digital cifrado en cualquier dispositivo.

La Fig. 1A muestra un sistema de DRM de la técnica anterior. Según se muestra en la Fig. 1A, dicho sistema de DRM incluye generalmente un Proveedor de Servicios (SP), un Emisor de Derechos, un terminal de DRM y un medio de almacenamiento. El Proveedor de Servicios y el Emisor de Derechos están usualmente asociados entre sí y pueden estar integrados entre sí. El medio de almacenamiento puede ser un almacén de red o diversos tipos de medios movibles. El terminal de DRM puede ser un programa de software o un hardware para solidificar la función del programa, que puede ser instalado en un dispositivo. Dicho dispositivo puede ser uno de diversos terminales digitales con una función de representación, tales como un teléfono móvil que tenga un reproductor, un Asistente Digital Personal (PDA), un equipo de sobremesa, un portátil, un MP3, un MP4, un lector de libros electrónicos, etc. La representación mencionada aquí incluye el significado de la lectura de los contenidos de textos digitales. La función de gestión de derechos digitales del dispositivo se logra mediante un módulo de DRM en el mismo.

La Fig. 1B muestra un diagrama de flujo de la DRM en la técnica anterior. Según se muestra en esta figura, en primer lugar, el dispositivo cliente obtiene los contenidos digitales, que incluyen el programa digital cifrado, del emisor de contenidos digitales. Un único contenido digital incluye no solamente el programa digital cifrado, sino también algunos otros componentes, tales como la cabecera. En donde el formato del programa digital puede ser audio, vídeo, texto u otros. La manera de distribuir u obtener los contenidos digitales puede ser implementada descargando desde sedes de la Red, emitiendo un disco compacto y distribuyendo contenidos digitales mediante la IPTV o la transmisión inalámbrica, etc. Como resultado, cuando se comienza a representar un programa, el dispositivo obtendrá la licencia para representar el programa desde el emisor de derechos, de acuerdo al aviso o instrucción de los contenidos digitales, y luego representa el programa en los contenidos digitales usando la licencia.

El artículo “Generación de clave de entorno hacia agentes despistados”, de Riordan y Schneier, 1998, referencia EPO XP001069390, introduce la noción de la generación de clave de entorno, en la que el material de la clave es construido a partir de ciertas clases de datos de entorno. Usando estas claves, los agentes podrían recibir mensajes cifrados que podrían descifrar solamente si algunas condiciones de entorno fuesen verdaderas. Los agentes con datos o código ejecutable cifrado usando tales claves podrían permanecer ignorantes de su propósito hasta que se satisfaga alguna condición de entorno. En la estructura básica, un agente tiene un mensaje de texto cifrado y un procedimiento para buscar en el entorno los datos necesarios para generar la clave.

No obstante, todavía hay algunas desventajas en las técnicas de DRM de la técnica anterior, que necesitan ser superadas. Por ejemplo, en el sistema de DRM basado en dispositivos, antes de conceder la licencia a un dispositivo, el emisor de derechos de autor comprobará si el dispositivo es compatible, sobre la base de una lista blanca o una lista negra, y, si el dispositivo no es compatible, el emisor de derechos no concede un derecho al dispositivo. En la DRM basada en personas, o híbrida, es necesario realizar en primer lugar una autenticación en tiempo real del dispositivo usado en la misma; pero cuando el dispositivo está fuera de línea, el centro de autenticación no puede emitir la licencia en tiempo real, o no puede autenticar el derecho de autor del dispositivo, por lo que es difícil identificar si el dispositivo está o no autorizado para representar los contenidos digitales.

Sumario de la invención

Es un objeto de la presente invención proporcionar un dispositivo y un procedimiento para la Gestión de Derechos Digitales, que permita identificar si el dispositivo tiene o no el derecho de representar el programa digital, independientemente de si el dispositivo está o no conectado con el servidor de autenticación.

De acuerdo a una realización de la invención, se proporciona un procedimiento para proporcionar contenidos digitales al usuario. El procedimiento comprende las siguientes etapas: codificar el programa digital para permitir que el programa digital sea asociado a un agente de autenticación, en donde dicho agente de autenticación incluye un bloque de código de programa, ejecutable por un dispositivo que puede representar dicho programa digital para autenticar la validez del dispositivo; y proporcionar un contenido digital que incluye dicho programa digital y dicho agente de autenticación a dicho dispositivo, de una manera en línea o fuera de línea.

En una realización, el programa digital es cifrado por un primer algoritmo de cifrado. La clave de descifrado CK del primer algoritmo de cifrado está cifrada por un segundo algoritmo de cifrado, y almacenada en el agente de autenticación. El bloque de código de programa también es operable para descifrar la clave cifrada CK después de que la validad del dispositivo ha superado la autenticación, a fin de obtener la clave CK y enviarla al módulo de DRM en el dispositivo, y dicho módulo de DRM descifra luego el programa digital cifrado en el contenido digital; o bien, después de que la validez del dispositivo ha superado la autenticación, el agente de autenticación envía la clave de descifrado de CK al módulo de DRM en el dispositivo, por lo que el módulo de DRM descifra la CK cifrada; finalmente, el módulo de DRM descifra el programa digital cifrado en el contenido original, por medio de la CK. Dicho módulo de DRM es un Módulo de Gestión de Derechos Digitales, pre-instalado en el dispositivo.

De acuerdo a otra realización de la invención, se proporciona un procedimiento para representar un contenido digital en un dispositivo. Dicho procedimiento comprende las siguientes etapas: obtener un contenido digital de un Proveedor de Servicios, incluyendo dicho contenido digital un programa digital y un agente de autenticación; ejecutar dicho agente de autenticación (301) para autenticar la validez del dispositivo; descifrar el programa digital (304) después de una autenticación exitosa; y representar el contenido digital descifrado.

De acuerdo a otra realización de la invención, se proporciona un procedimiento para autenticar fuera de línea la cualificación del dispositivo para representar el contenido digital, que comprende: incrustar el agente de autenticación en el contenido digital, de modo que, cuando dicho contenido digital es llevado a un dispositivo, el agente de autenticación se ejecuta y autentica si el dispositivo tiene la cualificación para representar el contenido digital.

De acuerdo a otra realización de la invención, se proporciona un dispositivo para representar un contenido digital. Dicho dispositivo comprende: un módulo de obtención para obtener el contenido digital de un Proveedor de Servicios, incluyendo dicho contenido digital un programa digital y un agente de autenticación; un módulo de DRM para ejecutar el agente de autenticación, para autenticar la validez del dispositivo y para descifrar el programa digital después de una autenticación exitosa; y un medio de representación para representar el programa digital descifrado.

Como puede verse, una ventaja prominente de la invención es que permite una autenticación de derechos digitales fuera de línea para identificar si el dispositivo es o no un representador válido, y tal autenticación puede ser realizada en el dispositivo, reduciendo así la carga en el servidor y posibilitando realizar la autenticación del derecho de autor en cualquier ubicación adecuada, sin estar restringido por la condición de la red.

Otros objetos y logros, junto con una comprensión más completa de la invención, devendrán evidentes y apreciados por referencia a la siguiente descripción y a las reivindicaciones, considerados conjuntamente con los dibujos adjuntos.

Descripción de los dibujos

La Fig. 1A muestra un dibujo esquemático de un esquema de DRM en la técnica anterior;
la Fig. 1B muestra un diagrama de flujo esquemático de la representación de un contenido de medios digitales cifrados en la técnica anterior;
la Fig. 2 muestra un dibujo esquemático de un sistema de DRM de acuerdo a una realización de la presente

invención;
la Fig. 3 muestra un dibujo esquemático de los componentes de un elemento de contenido digital, editado con el procedimiento de codificación de contenido digital de acuerdo a una realización de la presente invención;
la Fig. 4 muestra un dibujo esquemático de los componentes de la licencia, de acuerdo a una realización de la presente invención;
la Fig. 5A muestra un diagrama de flujo de la representación del contenido digital de acuerdo a una realización de la presente invención;
la Fig. 5B muestra un diagrama de flujo de la representación del contenido digital de acuerdo a una realización de la presente invención.

En toda la extensión de los dibujos, los mismos números de referencia indican las mismas características o funciones, similares o correspondientes.

Descripción detallada de la invención

De acuerdo a la presente invención, el esquema de cifrado usado en la invención se ilustra en primer lugar. Para hacer que la ilustración sea más clara y más concisa, se emplean las dos fórmulas siguientes:

$$Y = E_k(x) \quad (1)$$

donde E es un algoritmo de cifrado, x es el mensaje a cifrar, Y es el mensaje cifrado y k es la clave usada para cifrar el mensaje;

$$Y = D_k(x) \quad (2)$$

donde D es un algoritmo de descifrado, x es el mensaje a descifrar, y es el mensaje descifrado y k es la clave usada para descifrar el mensaje.

Tabla 1

Clave	Explicaciones de propiedades
CK	Clave de cifrado y descifrado de programa digital, para cifrar y descifrar el programa digital
(Pa, Pb)	Par de claves, para cifrar y descifrar la CK

Se usan dos grupos de claves en la invención, un grupo es la clave simétrica CK usada para cifrar el programa digital cuando el Proveedor de Servicios (SP) distribuye el contenido digital, y para descifrar inversamente en el dispositivo; y el otro grupo son las claves asimétricas (Pa, Pb) usadas para proteger la clave CK, lo que incluye una Clave de Cifrado de Clave (KEK) Pa y una Clave de Descifrado de Clave (KDK) Pb. Pa se usa para cifrar la CK mediante el algoritmo de cifrado $Y = E_{Pa}(CK)$, y Pb se usa para descifrar mediante la ecuación del algoritmo de descifrado $Y = D_{Pb}(x)$.

El sistema de protección de derechos digitales será ilustrado según lo siguiente, en base a las realizaciones.

Con referencia a la Fig. 2, el sistema de protección de derechos digitales 100 consiste en un Proveedor de Servicios (SP) 201 y un dispositivo 202.

El Proveedor de Servicios 201 recibe soporte de un servidor y comprende dos módulos funcionales, es decir, un módulo proveedor de derechos 2012 y un módulo proveedor de contenido digital 2011, para proporcionar, respectivamente, la licencia y el contenido digital. Dichos dos módulos pueden estar integrados dentro de un servidor, o pueden estar en dos servidores por separado. Dichos dos módulos no necesariamente proporcionan servicio simultáneamente. De acuerdo a la realización de la invención, un caso posible es que el módulo proveedor de contenido digital 2011 pueda proporcionar contenidos digitales en línea, mientras que el módulo proveedor de derechos 2012 proporciona la licencia fuera de línea; otro caso posible es que el módulo proveedor de contenido digital 2011 proporcione contenidos digitales fuera de línea, mientras que el módulo proveedor de derechos 2012 proporciona la licencia en línea; y un caso adicional es que tanto el módulo proveedor de contenido digital 2011 como el módulo proveedor de derechos 2012 proporcionen los contenidos digitales y la licencia en línea o fuera de línea. La licencia estipula las reglas para que el dispositivo represente los contenidos digitales. Además, el dispositivo 202 no puede representar los contenidos digitales sin una licencia adecuada.

La modalidad de provisión en línea incluye transmitir e intercambiar datos entre el Proveedor de Servicios y el dispositivo mediante Internet, la red de WAP, la transmisión inalámbrica, etc., conjuntamente con la técnica de interfaz inalámbrica. La modalidad de provisión fuera de línea incluye almacenar contenidos digitales en un disco magnético, un disco óptico u otros medios de almacenamiento extraíbles, y transferir los contenidos digitales de una manera convencional de transmisión.

El dispositivo 202 puede ser uno entre diversos tipos de terminales digitales con la función de representación, tales como un teléfono móvil con un reproductor, un Asistente Digital Personal (PD), un equipo de sobremesa, un portátil, un MP3, un MP4, un lector de libros electrónicos, etc. De acuerdo a una realización de la invención, el dispositivo 202 comprende además un módulo de almacenamiento 2023; alternativamente, el módulo de almacenamiento 2024 del dispositivo 202 tiene un código de identificación del dispositivo solidificado en el mismo, código de identificación que puede ser leído y usado para determinar la identidad del dispositivo 202. El módulo de almacenamiento 2024 también puede almacenar los contenidos digitales y la licencia obtenidos desde el Proveedor de Servicios 201.

La función de gestión de derechos digitales del dispositivo 202 es lograda por un módulo de DRM 2022 en el mismo. El módulo de DRM 2022 puede ser un programa de software independiente o una unidad acoplable de software, o puede ser un circuito de hardware. De acuerdo a una realización de la invención, se supone que el módulo de DRM 2022 es un programa de software independiente. En general, dicho módulo de DRM 2022 está proporcionado por el Proveedor de Servicios 201 o por otras personas o entidades autorizadas por el Proveedor de Servicios 201. Un código de identificación está pre-dispuesto en el módulo de DRM 2022 para determinar la identidad del módulo de DRM 2022. Esta identidad puede estar asociada a la identidad del dispositivo de representación de contenido digital. Alternativamente, el módulo de DRM 2022 puede estar dispuesto de acuerdo a las necesidades, para autenticar por iniciativa la validez del contenido digital y para representar solamente el contenido digital que supera la autenticación de validez.

De acuerdo a una realización de la invención, entre los contenidos digitales proporcionados por el Proveedor de Servicios 201, cada contenido digital 300 incluye no solamente el programa digital a representar, sino también un agente de autenticación incrustado 301. Dicho agente de autenticación 301 es, de hecho, un módulo de programa de software operable en el dispositivo 202, que se usa para autenticar (haciéndolo para el Proveedor de Servicios 201) si el dispositivo de representación 202 (módulo de DRM) es o no un usuario válido (usuario autorizado). En donde esto puede ser realizado autenticando si el código de identificación del módulo de DRM 2022 en el dispositivo 202 pertenece o no a uno entre los usuarios válidos. Por tanto, se logra la función de protección de derechos digitales fuera de línea.

De acuerdo a una realización de la invención, el dispositivo 202 comprende un módulo de obtención 2021 para obtener los contenidos digitales proporcionados por el Proveedor de Servicios 201 y el Agente de Autenticación incrustado en los contenidos digitales.

De acuerdo a una realización de la invención, el dispositivo 202 comprende además un módulo de representación (reproducción) 2023 para representar (reproducir) el programa digital, de acuerdo a la licencia obtenida por el dispositivo 202, dicho módulo de representación 2023 puede ser un medio de descodificación de audio / vídeo tal como un descodificador de MEPG-2, MEPG-4, etc., y el derecho de representación está limitado por la licencia.

De acuerdo a una realización de la invención, cuando el Proveedor de Servicios 201 distribuye contenidos de programas digitales de acuerdo a la demanda del usuario (en línea o fuera de línea), normalmente necesita convertir primero el programa digital a un formato estándar, tal como wma, asf, wmv, etc., y cifrar el programa digital usando un algoritmo adecuado. En términos generales, a fin de no provocar demasiada carga en el cálculo, se usa normalmente la criptografía simétrica, es decir, se usa la misma clave tanto para el cifrado como para el descifrado. Por supuesto, también pueden usarse otras formas de cifrado. Además de cifrar el programa digital, también se añaden otros datos relevantes al contenido de programa digital, luego se hace una rúbrica digital y el programa digital se empaqueta en un único contenido digital. Según se describe más adelante, el procedimiento de codificación usado cuando el Proveedor de Servicios 201 proporciona contenidos digitales se explica en detalle con referencia a la Fig. 3.

La Fig. 3 muestra un elemento de contenido digital editado por el procedimiento de codificación de contenido digital, de acuerdo a una realización de la presente invención. Según se muestra en la figura, un único contenido digital 300 incluye un programa digital cifrado 304, un agente de autenticación 301, un Identificador de contenido 302 y algunos otros componentes optativos. Alternativamente, incluye además una rúbrica digital 303. El Identificador de contenido 302 se usa para indicar el número de serie del contenido digital. La rúbrica digital 303 puede indicar la identidad del emisor del contenido digital y proteger la integridad del contenido. Si el contenido digital 300 está alterado, será identificado autenticando la rúbrica 303.

Además, de acuerdo a la Fig. 3, el agente de autenticación 301 comprende un Identificador de agente de autenticación 3011, una parte de código de programa 3012, una clave cifrada CK 3013 y una rúbrica digital 3014, etc. El Identificador de agente de autenticación 3011 indica el número de serie del agente de autenticación 301, para su asociación con el contenido de programa relacionado. La rúbrica digital 3014 puede indicar la identidad del emisor del agente de autenticación 301 y proteger la integridad del agente de autenticación 301, etc. La clave CK es una clave para descifrar el contenido digital cifrado. El código de programa 3012 puede realizar y lograr dos funciones: una es autenticar la validez del dispositivo de representación 202 usando la lista negra o lista blanca incrustada, la otra es descifrar la clave cifrada CK 3013 o entregar la clave de descifrado de la clave CK del módulo de DRM 2022, que descifra la clave CK. Tal descifrado es realizado mediante la Clave de Descifrado de Clave Pb,

usando la fórmula del algoritmo de descifrado. Alternativamente, el agente de autenticación 301 también comprende una Clave de Descifrado de Clave Pb.

La Fig. 4 muestra los componentes esquemáticos de la licencia 400, de acuerdo a una realización de la presente invención. La Licencia 400 proporcionada por el Proveedor de Servicios incluye principalmente un Identificador de licencia 401, un Identificador de contenido 402, una restricción de representación 403, la información de periodo válido 404 y una rúbrica digital 405. Pueden estar presentes otras partes optativas. El Identificador de licencia 401 indica el número de serie de la licencia 400, el Identificador de contenido 402 indica el programa de contenido correspondiente a dicha licencia 400. La información de periodo válido 404 especifica el periodo de validez de la licencia 400, y la rúbrica digital 405 indica la identidad del emisor y / o la fecha de emisión de la licencia 400, y protege la integridad de la licencia.

La realización de la función de Gestión de Derechos Digitales durante la representación del programa digital en el dispositivo está específicamente descrita según lo siguiente, con referencia a las Figs. 5A y 5B.

El dispositivo está pre-instalado en un módulo de DRM, que está usualmente proporcionado por el Proveedor de Servicios (facilitador) que proporciona los contenidos digitales. Los módulos de DRM proporcionados por distintos facilitadores pueden variar, es decir, el módulo de DRM proporcionado por un Proveedor de Servicios puede solamente ser usado para representar los contenidos digitales proporcionados por dicho proveedor de servicios; o varios facilitadores, tal vez, comparten un módulo de DRM compatible, y luego el módulo de DRM proporcionado por un Proveedor de Servicios puede representar los contenidos digitales proporcionados por varios Proveedores de Servicios (SP).

El módulo de DRM en el dispositivo necesita obtener una licencia, para representar los contenidos digitales, de un Proveedor de Servicios, a fin de representar los contenidos digitales obtenidos del Proveedor de Servicios. Alternativamente, la licencia puede ser obtenida por descarga desde el Proveedor de Servicios, o por otras formas factibles, de acuerdo a instrucciones, tales como comprando un disco óptico que tenga la licencia almacenada en el mismo. El usuario puede descargar la licencia obtenida y el programa de software de DRM al dispositivo, o incluso descargarlos a un medio de almacenamiento portátil (como un disco Universal) y llevarlo consigo para usar la licencia en muchos dispositivos. La licencia especifica el derecho de representación del módulo de DRM, es decir, la regla de representación (reproducción).

La Clave de Descifrado de Clave Pb puede ser almacenada en el Agente de Autenticación, o en el módulo de almacenamiento del dispositivo.

De acuerdo a una realización de la invención, en el caso en que la Clave de Descifrado de Clave Pb es almacenada en al Agente de Autenticación, según se muestra en la Fig. 5A, el proceso del uso del dispositivo para obtener y representar los contenidos digitales incluye las siguientes etapas:

Etapa S501: obtener los contenidos digitales.

El usuario del dispositivo 202 obtiene el contenido digital deseado 300 desde el Proveedor de Servicios 201, en línea o fuera de línea.

Cuando el usuario halla un programa digital que le gusta, mediante la red u otro anuncio, puede obtener el contenido digital que contiene dicho programa digital en línea o fuera de línea, por ejemplo, por descarga desde la red, o comprando un disco óptico, etc. El programa digital en dicho contenido digital está cifrado. En el sector del Proveedor de Servicios, durante el proceso en el cual los programas digitales son empaquetados en contenido digital, además de cifrar los programas digitales, se añaden algunos otros datos a los mismos, incluyendo el agente de autenticación, el Identificador, etc., Luego el Proveedor de Servicios encapsula el contenido digital y genera una rúbrica digital.

Alternativamente, después de que el módulo de DRM 2022 lee el contenido digital 300, puede ser interrogado en cuanto a si la licencia 400 para representar dicho contenido digital ha sido obtenida o no; si la licencia no ha sido obtenida, el dispositivo debería obtener primero la licencia del Proveedor de Servicios, de acuerdo a la interrogación, y luego avanzar a la etapa S502; si la licencia ha sido obtenida, se le induce a leer la licencia 400 y se omite la etapa S502.

Etapa S502: obtener la licencia.

El usuario necesita obtener la licencia 400 para representar el contenido digital, y esto es requerido por el módulo de DRM 2022 en el dispositivo. La licencia 400 puede ser una licencia especial para uno o varios elementos de contenidos digitales, o puede ser una licencia universal para todos los contenidos digitales proporcionados por el servidor. Preferiblemente, el contenido digital registra la sede de la Red desde la cual puede ser descargada la licencia, para que el dispositivo del usuario pueda descargar la licencia desde la sede de la Red. La licencia también

puede ser obtenida fuera de línea, tal como por estar almacenada en un medio. En donde la licencia especifica la restricción para la representación, tal como los momentos de representación, la hora de representación, si el contenido digital puede ser guardado o no, si el contenido digital puede o no ser impreso, si el contenido digital puede ser modificado o no, y si una toma de fotografía de intercepción dispone o no de soporte, etc.

Para el Proveedor de Servicios que se lucra con la Gestión de Derechos Digitales, la obtención de la licencia puede ser una transacción, y puede ser requerido el pago en línea o fuera de línea.

Etapa S503: autenticar la validez.

Alternativamente, el dispositivo 202 autentica en primer lugar si el contenido digital obtenido 300 ha sido o no alterado alguna vez, incluso que el módulo de DRM 2022 extraiga la rúbrica digital del contenido digital, y la rúbrica digital del agente de autenticación, desde el contenido digital obtenido para autenticar, a fin de determinar si el contenido digital per se, y el agente de autenticación, son válidos o no, es decir, si han sido o no ilegalmente alterados y si es o no el contenido digital proporcionado por el Proveedor de Servicios. El objeto de esta operación es permitir al módulo de DRM 2022 del dispositivo 202 representar solamente el contenido digital 300 obtenido desde el Proveedor de Servicios 201. Dado que el módulo de DRM 2022 también es generalmente proporcionado por el Proveedor de Servicios 201, esto puede urgir al usuario del dispositivo para obtener el contenido digital legal desde el Proveedor de Servicios.

El programa 3012 del agente de autenticación se ejecuta en el dispositivo 202, y el agente de autenticación 301 comienza a autenticar si el dispositivo 202 es o no un dispositivo válido de representación. Esto puede ser realizado autenticando si el módulo de DRM en el dispositivo es válido o leyendo el número de serie inherente del dispositivo en el dispositivo. El procedimiento de lista blanca o de lista negra se usa para la autenticación (por supuesto, no están excluidos otros procedimientos para determinar la validez del dispositivo), o ambos elementos pueden ser autenticados. El agente de autenticación puede almacenar una tal lista blanca o lista negra. Con el desarrollo y la actualización del dispositivo, al distribuir contenidos digitales, el Proveedor de Servicios puede actualizar continuamente la lista negra, o la lista blanca, incrustada.

Si la autenticación es exitosa, lo que indica que el dispositivo (es decir, el módulo de DRM) es legalmente adecuado o pertenece a un ámbito especificado de dispositivos, luego se llega a la siguiente etapa.

Etapa 504: descifrado de clave – descifrar para obtener la CK usando Pb

El agente de autenticación 2021 extrae la clave cifrada CK (3013) y usa la fórmula del algoritmo de descifrado Ck = D_{Pb} (CK cifrada) para descifrar la clave cifrada CK. En donde la Clave de Descifrado de Clave Pb se añade al agente de autenticación cuando el Proveedor de Servicios distribuye el contenido digital. Luego, la clave CK se envía al módulo de DRM. En el uso práctico, el algoritmo de descifrado de clave D difícilmente puede ser compilado inversamente, por lo que se considera seguro.

Etapa 505: el módulo de DRM 2022 usa la clave CK para descifrar el programa digital cifrado. En general, se cree que los algoritmos de cifrado usados normalmente han sido ya pre-formulados en el módulo de DRM, e incluso pueden recibir soporte de dispositivos especiales de hardware. Posiblemente, el fichero de cabecera del fichero de contenido digital define los algoritmos de cifrado y descifrado digital usados por el contenido. El módulo de DRM descifra el contenido digital mediante la CK obtenida en la etapa 504, usando el algoritmo definido en el fichero de cabecera del contenido digital.

El módulo de DRM lee la licencia y envía el programa digital al núcleo de representación, tal como el núcleo de representación de MEPG-2, MEPG-4, el reproductor de Flash, o el lector de texto, para ser representado. El derecho de representación está limitado por la licencia.

De acuerdo a una realización de la invención donde la Clave de Descifrado de Clave está incluida en la licencia, con referencia a la Fig. 5B, el proceso de representación del contenido digital por parte del dispositivo difiere del de la realización previa, en cuando a que, en el proceso de descifrado de clave de la etapa S504', el agente de autenticación lee la Clave de Descifrado de Clave Pb pre-dispuesta, desde el medio de almacenamiento fijo del dispositivo, y luego obtiene la CK usando el algoritmo de descifrado de clave. Mientras que el resto de las etapas son esencialmente las mismas.

Además, la rúbrica digital precitada y la rúbrica de autenticación pueden usar diversas formas de generar una rúbrica, incluyendo la rúbrica de clave pública. En la presente invención, a fin de simplificar la solución, se usa la rúbrica de clave pública, pero esto no significa excluir otras técnicas de rúbrica electrónica. Con respecto a la rúbrica de clave pública, la clave y al algoritmo para autenticar la rúbrica pueden estar pre-solidificadas en el módulo de DRM, y el módulo de DRM autentica la rúbrica digital usando el algoritmo y la clave. Si la rúbrica digital es válida, significa que el contenido está proporcionado por el Proveedor de Servicios y no está alterado.

Los expertos en la técnica entenderán que cualquier diagrama de flujo y los dibujos cualesquiera de los componentes modulares funcionales, incluidos en la solución técnica divulgada en la invención, representan diversos procesamientos distintos que pueden ser realizados esencialmente en un medio legible por ordenador, para que puedan ser ejecutados por un ordenador o procesador, independientemente de si un ordenador o procesador de ese tipo ha sido explícitamente indicado o no. Se entenderá que la invención no está limitada a las realizaciones descritas anteriormente y a la mejora para las mismas. Los expertos en la técnica podrán hacer muchas variaciones y mejoras sin apartarse del concepto y del ámbito definidos por las reivindicaciones adjuntas. En las reivindicaciones, todo signo de referencia colocado entre paréntesis no será interpretado como limitador de la reivindicación. La palabra “comprende” no excluye la presencia de elementos o etapas distintos a los enumerados en una reivindicación. La palabra “un” o “uno”, precediendo a un elemento, no excluye la presencia de una pluralidad de tales elementos. La invención puede ser implementada por medio de hardware que comprende varios elementos distintos y / o por medio de un procesador adecuadamente programado. En la reivindicación del dispositivo que enumera varios medios, varios de estos medios pueden ser realizados por un mismo elemento de hardware. El mero hecho de que ciertas medidas sean reveladas en reivindicaciones dependientes mutuamente distintas no indica que una combinación de estas medidas no pueda ser usada con ventaja.

REIVINDICACIONES

1. Un procedimiento para proporcionar una autorización de programa digital (304) a un dispositivo (202) que puede representar dicho programa digital (304), que comprende las etapas de:

- codificar el programa digital (304) para asociar dicho programa digital (304) a un agente de autenticación (301), en donde dicho agente de autenticación (301) incluye un código de programa (3012) ejecutable por el dispositivo (202) para autenticar la validez del dispositivo (202);
- empaquetar juntos el programa digital (304) y el agente de autenticación (301) en un único contenido digital, y
- proporcionar el contenido digital (300) que incluye dicho programa digital (304) y dicho agente de autenticación (301) a dicho dispositivo (202), en el que
- el programa digital (304) está cifrado por un primer algoritmo de cifrado, y la clave de descifrado del primer algoritmo de cifrado está cifrada por un segundo algoritmo de cifrado, dando como resultado una clave de descifrado cifrada (3013), y almacenada en el agente de autenticación (301), y

el código de programa (3012) también es operable para descifrar la clave cifrada (3013) si la validez del dispositivo (202) ha superado la autenticación, a fin de obtener la clave de descifrado del primer algoritmo de cifrado.

2. El procedimiento de la Reivindicación 1, en el que el agente de autenticación (301) comprende un identificador de agente de autenticación (3011) que indica un número de serie del agente de autenticación (301) para asociar el agente de autenticación al programa digital.

3. El procedimiento de la reivindicación 2, en el que el código de programa (3012) también es operable para enviar la clave cifrada (3013) a un módulo de DRM (2022) en el dispositivo (202), y dicho módulo de DRM descifra luego el programa digital cifrado (304) en el contenido digital (300); en el que el módulo de DRM (2022) es un Módulo de Gestión de Derechos Digitales pre-instalado en el dispositivo.

4. El procedimiento de la reivindicación 3, en el que

- el agente de autenticación (301) incluye además una Clave de Descifrado de Clave para descifrar la clave cifrada (3013);
- el código de programa (3012) en el agente de autenticación (301) es operable para extraer la Clave de Descifrado de Clave desde el agente de autenticación (301) y para descifrar la clave cifrada CK (3013) de acuerdo a un algoritmo de descifrado prefijado, correspondiente al segundo algoritmo de cifrado.

5. El procedimiento de la Reivindicación 4, en el que la clave cifrada CK (3013) ha sido cifrada usando una clave de cifrado de clave (KEK, Pa) asimétrica, descifrando el agente de autenticación la clave de descifrado cifrada (CK), usando una clave de descifrado de clave (KDK, Pb) asimétrica.

6. El procedimiento de la reivindicación 3, en el que, después de obtener el programa digital descodificado, el módulo de DRM (2022) controla la representación del programa digital de acuerdo a la licencia pre-obtenida (400).

7. Un procedimiento para representar un contenido digital en un dispositivo (202), que comprende las etapas de:

(a) obtener el contenido digital (300) desde un Proveedor de Servicios (201), siendo dicho contenido digital (300) un único contenido digital en el que están empaquetados un programa digital (304) y un agente de autenticación (301);
(b) ejecutar dicho agente de autenticación (301) para autenticar la validez del dispositivo;
(c) descifrar el programa digital (304) después de una autenticación exitosa; y
(d) representar el programa digital descifrado (304),

estando el programa digital (304) cifrado por un primer algoritmo de cifrado, y estando cifrada la clave de descifrado del primer algoritmo de cifrado por un segundo algoritmo de cifrado, y almacenada en el agente de autenticación (301).

8. El procedimiento de la reivindicación 7, en el que el programa digital (304) está cifrado por un primer algoritmo de cifrado, y la clave de descifrado del mismo está incrustada en el agente de autenticación (301) después de ser cifrada por un segundo algoritmo de cifrado.

9. El procedimiento de la reivindicación 7, en el que, en la etapa (b), el agente de autenticación (301) autentica la validez del dispositivo comparando el Identificador prefijado en el dispositivo y una lista blanca, o una lista negra, incrustada en el agente de autenticación (301).

10. El procedimiento de la reivindicación 8, en el que la etapa (b) incluye una etapa de invocar una Clave de Descifrado de Clave, incrustada en el agente de autenticación (301), para descifrar la clave cifrada (3013).

11. El procedimiento de la reivindicación 8, en el que la etapa (b) incluye una etapa de invocar desde el dispositivo

una Clave de Descifrado de Clave que está pre-almacenada en el mismo, para descifrar la clave cifrada (3013).

12. Un procedimiento para autenticar la validez del dispositivo que representa el contenido digital, que comprende un procedimiento para proporcionar una autorización de un programa digital (304), de acuerdo a una cualquiera de las reivindicaciones 1 a 11, procedimiento que comprende:

incrustar un agente de autenticación (301) en el contenido digital (300), de modo que, cuando dicho contenido digital sea llevado a un dispositivo (202), el agente de autenticación (301) se ejecute y autentique si el dispositivo (202) tiene o no una cualificación para representar el contenido digital (300).

13. El procedimiento de la reivindicación 12, en el que

- el contenido digital (300) incluye el programa digital (304), y
- el agente de autenticación (301) incluye el código de programa (3012) que es operable para comparar y autenticar el código de identificación del módulo de DRM (2022) que se ejecuta en el dispositivo (202).

14. El procedimiento de la reivindicación 12, en el que

- el agente de autenticación (301) incluye una lista para comparar con el código de identificación prefijado en el módulo de almacenamiento del dispositivo y / o el código de identificación prefijado en el módulo de DRM (2022), y
- el código de programa (3012) en el agente de autenticación (301) se ejecuta para comparar el código de identificación del dispositivo con la lista, a fin de determinar si el dispositivo y / o el módulo de DRM (2022) en el mismo son o no válidos.

15. Un dispositivo (202) para representar un contenido digital, que comprende:

- un módulo de obtención (2021) para obtener el contenido digital (300) desde un Proveedor de Servicios (201), incluyendo dicho contenido digital (300) un programa digital (304) y un agente de autenticación (301); estando el programa digital (304) codificado para asociar el programa digital (304) al agente de autenticación (301), en donde dicho agente de autenticación (301) incluye un código de programa (3012) para autenticar la validez del dispositivo (202), estando empaquetados juntos el programa digital (304) y el agente de autenticación (301) en dicho contenido digital único, estando el programa digital (304) cifrado por un primer algoritmo de cifrado, y estando cifrada la clave de descifrado del primer algoritmo de cifrado por un segundo algoritmo de cifrado, dando como resultado una clave de descifrado cifrada (3013), y almacenada en el agente de autenticación (301),
- un módulo de DRM (2022) para ejecutar el agente de autenticación (301), para autenticar la validez del dispositivo (202) y, si tal autenticación fuera exitosa, descifrar la clave cifrada (3013) para obtener la clave de descifrado del primer algoritmo de cifrado, y usar la clave de descifrado para descifrar el programa digital (304); y
- un módulo de representación (2023) para representar el programa digital descifrado (304).

16. El dispositivo de la reivindicación 15, en el que el contenido digital (300) incluye además un Identificador de contenido (302) y una rúbrica digital de contenido (303) que indica información tal como la identidad del emisor del contenido digital (201) y la hora, y protege la integridad de los datos.

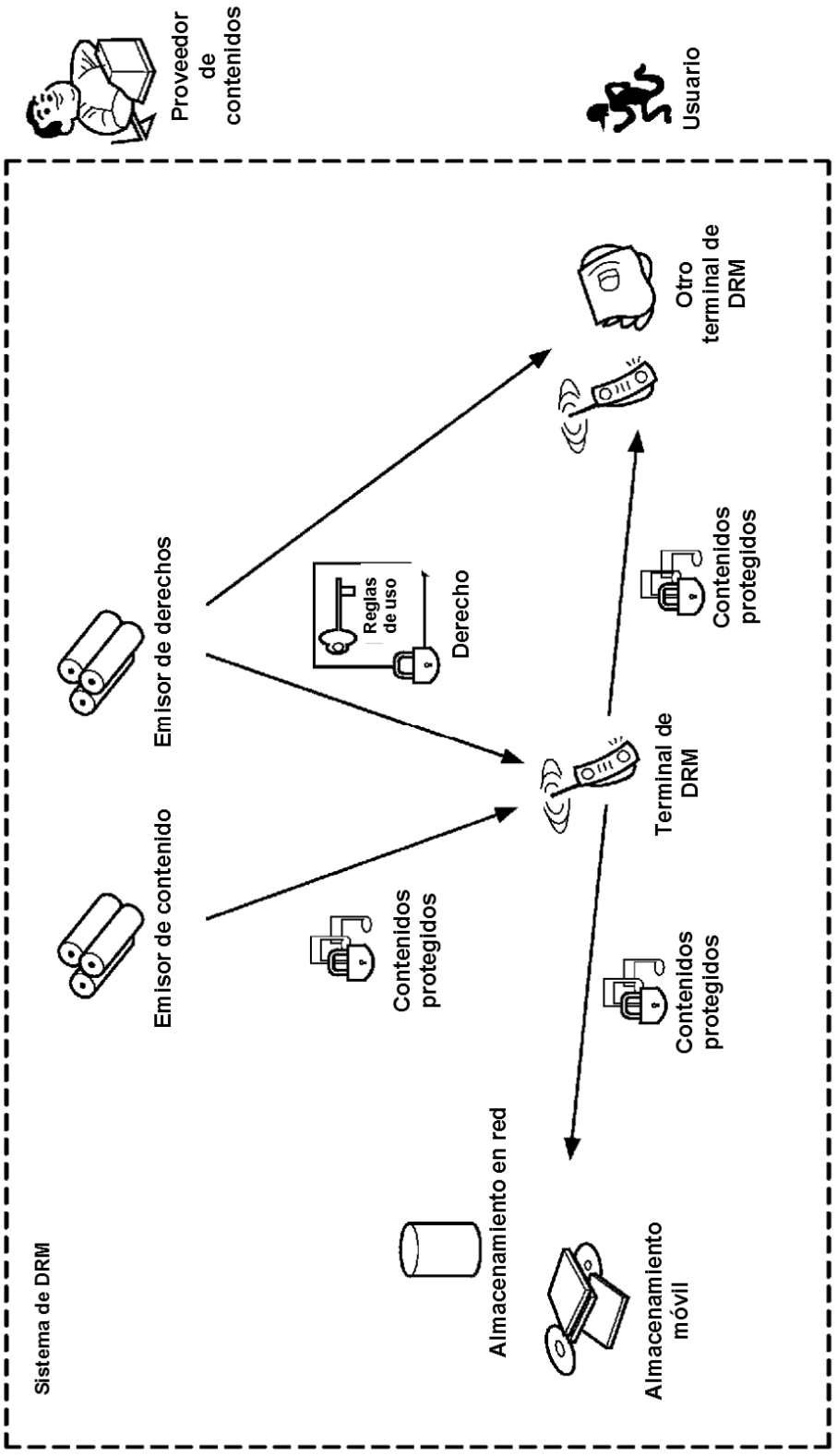
Proveedor de contenidos
Usuario
Sistema de DRM
Emisor de derechos
Emisor de contenido
Reglas de uso
Derecho
Contenidos protegidos
Contenidos protegidos
Contenidos protegidos
Otro terminal de DRM
Terminal de DRM
Almacenamiento en red
Almacenamiento móvil

FIG. 1A

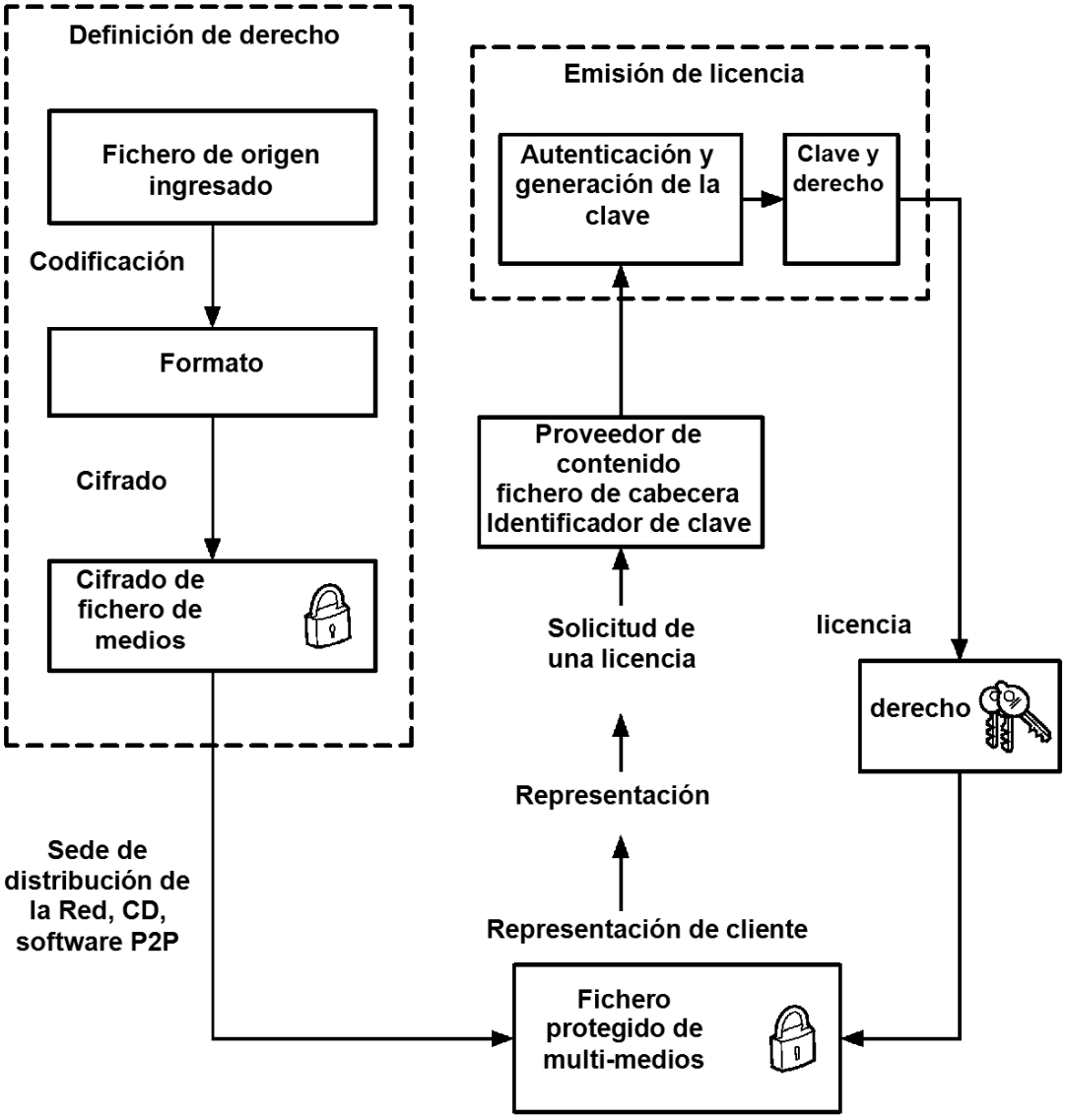
Definición de derecho
Fichero de origen ingresado
Codificación
Formato
Cifrado
Cifrado de fichero de medios
Sede de distribución de la Red, CD, software P2P
Emisión de licencia
Autenticación y generación de la clave
Clave y derecho
Proveedor de contenido fichero de cabecera Identificador de clave
Solicitud de una licencia
licencia
derecho
Representación
Representación de cliente
Fichero protegido de multi-medios

FIG. 1B

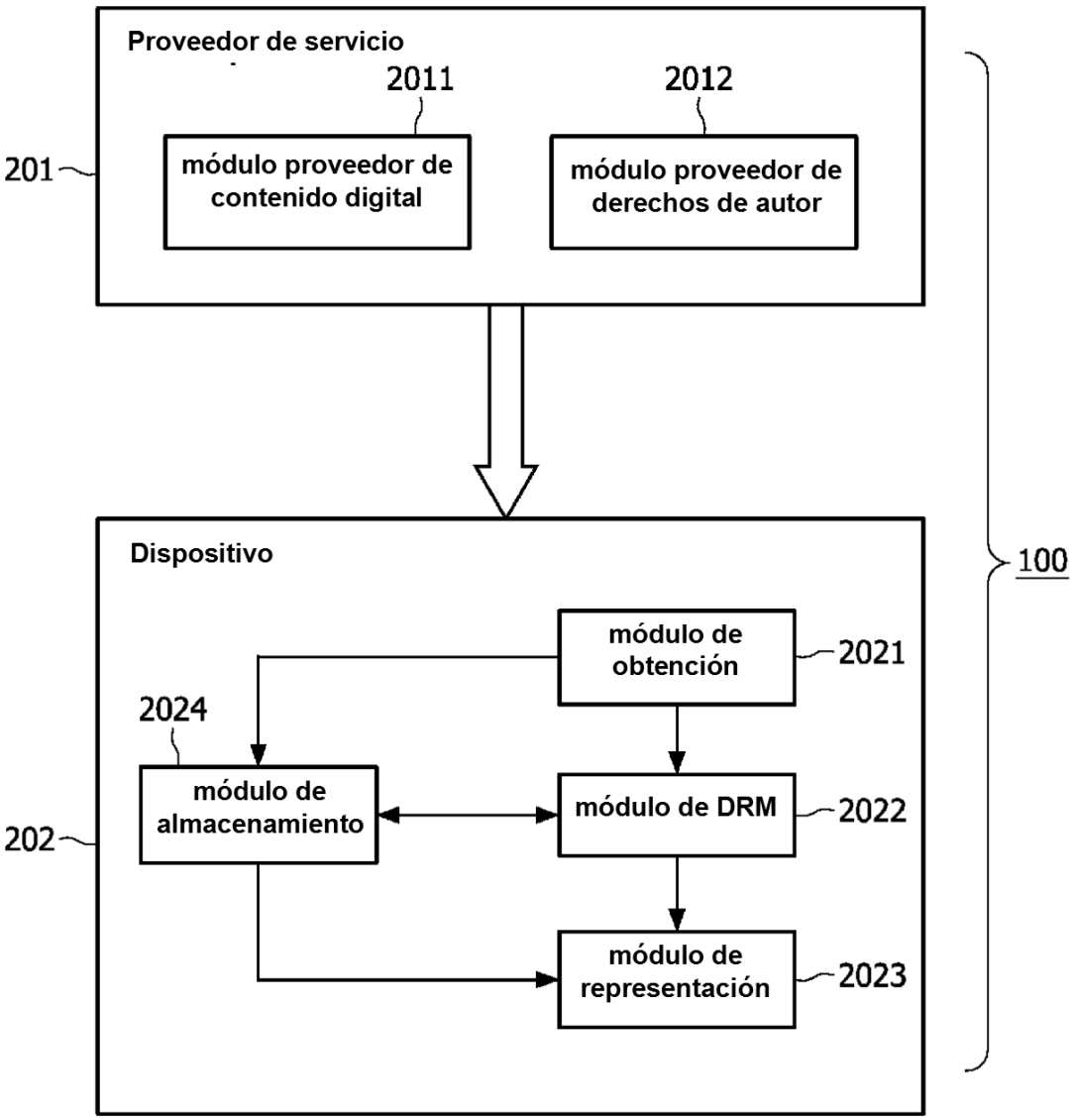
Proveedor de servicio
2011
2012
201
módulo proveedor de contenido digital
módulo proveedor de derechos de autor
Dispositivo
módulo de obtención
2021
2024
módulo de almacenamiento
módulo de DRM
2022
202
módulo de representación
2023
100

FIG. 2

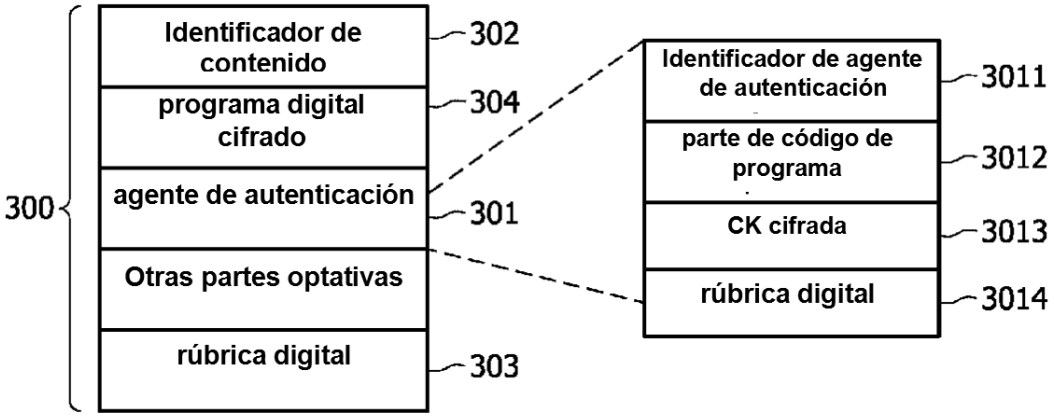
300
Identificador de contenido
302
programa digital cifrado
304
agente de autenticación
301
Otras partes optativas
rúbrica digital
303
Identificador de agente de autenticación
3011
parte de código de programa
3012
CK cifrada
3013
rúbrica digital
3014

FIG. 3

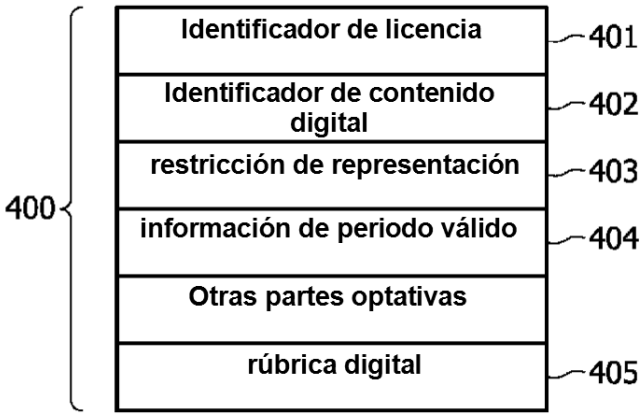
400
Identificador de licencia
401
Identificador de contenido digital
402
restricción de representación
403
información de periodo válido
404
Otras partes optativas
rúbrica digital
405

FIG. 4

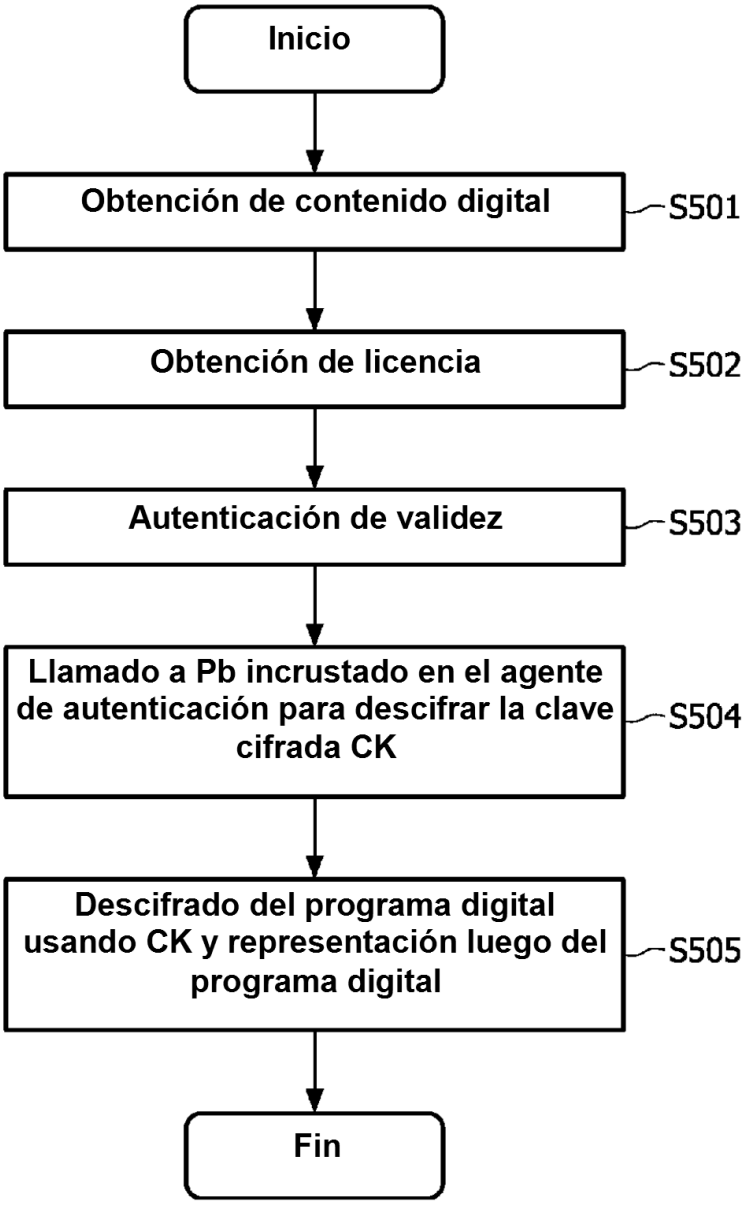
Inicio
Obtención de contenido digital
S501
Obtención de licencia
S502
Autenticación de validez
S503
Llamado a Pb incrustado en el agente de autenticación para descifrar la clave cifrada CK
S504
Descifrado del programa digital usando CK y representación luego del programa digital
S505
Fin

FIG. 5A

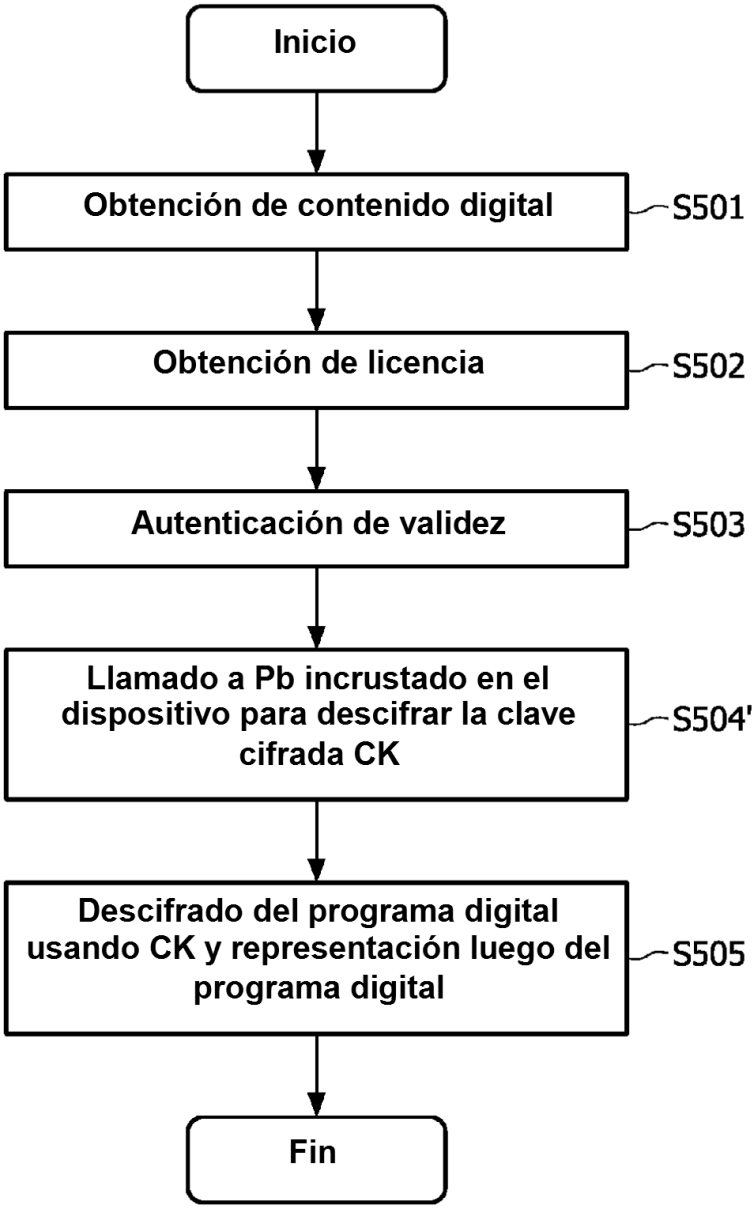
Inicio
Obtención de contenido digital
S501
Obtención de licencia
S502
Autenticación de validez
S503
Llamado a Pb incrustado en el dispositivo para descifrar la clave cifrada CK
S504'
Descifrado del programa digital usando CK y representación luego del programa digital
S505
Fin

FIG. 5B