(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 397 844**

(51) Int. CI.:

G06F 21/00 (2006.01)
H04L 9/08 (2006.01)
H04N 7/167 (2011.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **01.03.2005 E 05707671 (3)**

(97) Fecha y número de publicación de la concesión europea: **24.10.2012 EP 1769604**

(54) Título: **Sistema y procedimiento para la gestión de derechos digitales de un contenido electrónico**

(30) Prioridad:

22.03.2004 US 555250 P
26.08.2004 US 926689

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
11.03.2013

(73) Titular/es:

TELEFONAKTIEBOLAGET LM ERICSSON (PUBL) (100.0%)
PATENT UNIT
164 83 STOCKHOLM, SE

(72) Inventor/es:

BJÖRKENGREN, ULF y
STAHL, PER

(74) Agente/Representante:

DE ELZABURU MÁRQUEZ, Alberto

DESCRIPCIÓN

Sistema y procedimiento para la gestión de derechos digitales de un contenido electrónico.

La invención se refiere a la seguridad de un contenido electrónico. Más particularmente, la invención se refiere a la gestión de derechos digitales de un contenido electrónico.

Cada vez más información es transmitida electrónicamente en formato digital. Prácticamente cualquier cosa que puede ser representada por medio de palabras, números, gráficos, información de audio o de vídeo, o un sistema de comandos e instrucciones puede ser formateada en información electrónica digital, denominada también "contenido digital" o simplemente "contenido". Los aparatos electrónicos de diversos tipos están todos interconectados, proporcionando a sus usuarios la posibilidad de realizar una gran diversidad de tareas, tales como telecomunicaciones, transacciones financieras, operaciones comerciales, investigación y transacciones relacionadas con el entretenimiento.

Un problema fundamental para los proveedores de contenidos digitales es ampliar su capacidad de controlar el uso de información de propiedad privada, tal como contenido protegido por derechos de autor. Frecuentemente, los proveedores de contenidos quieren limitar el uso de los contenidos a actividades y en cantidades autorizadas. Por ejemplo, los proveedores de contenidos comerciales se preocupan de garantizar que reciben una compensación adecuada por el uso de los contenidos.

Los proveedores y distribuidores de contenidos han empleado una serie de mecanismos de protección de derechos para impedir el uso no autorizado de su contenido. Entre los mismos, se encuentra la gestión de derechos digitales (Digital Rights Management, DRM). DRM se refiere a la concesión de licencias y al control de la distribución y el uso de contenidos digitales. En general, los sistemas DRM distribuyen contenido digital en una forma cifrada. Un conjunto de derechos están asociados con el contenido, y un usuario podrá descifrarlo sólo después de adquirir los derechos para acceder a una pieza protegida del contenido digital. Actualmente hay especificaciones DRM encontradas, que incluyen Alianza Móvil Abierta (Open Mobile Alliance, DRM OMA), dispositivos de Windows Media (Windows Media Device, WM D-DRM), y otros.

La distribución de contenidos DRM se está generalizando cada vez más conforme más dispositivos, tales como teléfonos celulares y asistentes personales digitales (PDAs) tienen capacidad DRM. Según la arquitectura de software convencional, tal como se ve desde una vista de alto nivel del sistema, el software para los dispositivos es una pieza monolítica. Por ejemplo, algunas soluciones DRM actuales proponen la implementación de una función DRM en el software contenido en el dispositivo de mano. Más particularmente, algunas soluciones DRM convencionales requieren el uso de un "dispositivo de reproducción DRM" dedicado, tal como un navegador, un reproductor multimedia, etc.

Un enfoque alternativo consiste en dividir el software en una parte de plataforma, que tiene un dominio de software de plataforma, que incluye los componentes de software y servicios fundamentales; y una parte de aplicación, que tiene un dominio de software de aplicación, que incluye componentes de software que están relacionados más estrechamente con características específicas del dispositivo. Un ejemplo de dicho un sistema se describe en la solicitud de patente US2004205333 “Method and System for Digital Rights Management”, presentada el 14 de Abril de 2003. En la descripción siguiente, se asume que se usa una arquitectura de software que tiene partes de plataforma y de aplicación.

La Figura 1 ilustra un modelo básico para proporcionar contenido usando DRM. Un proveedor 100 de contenidos crea y empaqueta contenido digital según la especificación DRM y establece uno o más conjuntos de derechos de uso (o reglas) y los costos de uso asociados, que están asociados con los diversos usos posibles de los contenidos (por ejemplo, reproducción, impresión, copia, distribución, etc.) y el número de veces permitido, o período de tiempo, en el que el contenido está disponible. El contenido es transferido a un distribuidor 110 que lo hace disponible para los usuarios 120, por ejemplo, en el sitio web, a modo de escaparate virtual, de un distribuidor. A continuación, un usuario 120, que utiliza un equipo de usuario (EU), puede navegar por el contenido disponible del distribuidor y puede seleccionar el contenido de interés para el usuario 120, seleccionando también uno de los derechos de uso definidos para el contenido (teniendo en cuenta los costes de uso asociados). El usuario 120 realiza el pago adecuado al distribuidor 110 para el contenido/uso seleccionado, momento en el que los derechos de contenido y de uso pueden ser transferidos al EU, que puede ser un terminal móvil, una PDA, un reproductor multimedia u otro dispositivo similar capaz de reproducir el contenido. A continuación, el EU puede reproducir el contenido según las normas de uso para hacerlo disponible para su uso por el usuario 120 según las normas de uso. En algunos casos, los derechos se conceden mediante el pago a un intermediario (no mostrado), tal como un agente de pago, el cual indica, a continuación, al distribuidor 110 que suministre el contenido.

Los datos relacionados con DRM pueden ser definidos, en general, como dos entidades (un contenedor de contenidos y una licencia) que pueden ser transferidos como un solo paquete físico o como dos paquetes físicos separados. El último caso es más flexible ya que puede obtenerse una licencia nueva sin reenviar el contenido completo y se consigue un nivel

de seguridad más alto cuando el contenido y la licencia no se transfieren juntos. Si el contenedor de contenidos y la licencia se transfieren por separado, cada uno de ellos debe incluir información de vinculación.

El contenedor de contenidos comprende el contenido real que el usuario desea reproducir, que está típicamente en una forma cifrada para su protección contra el uso no autorizado. La licencia incluye generalmente los derechos de uso del contenido asociado, por ejemplo, un objeto de derechos, y una clave, o parte o la totalidad de la información necesaria para generar una clave, necesaria para el descifrado del contenido.

Tal como se ha indicado anteriormente, los derechos de uso definen las condiciones que se aplican a la reproducción de los contenidos. Para permitir una expresión flexible y extensible de los derechos de uso, se han desarrollado lenguajes de expresión de derechos (LED) especiales. Dos de las alternativas LED dominantes en la actualidad se llaman lenguaje de marcado extensible de derechos (Extensible Rights Markup Language, XrML) y lenguaje abierto de derechos digitales (Open Rights Language, ODRL), ambos de los cuales están basados en lenguaje de marcado extensible (Extensible Markup Language, XML).

Las plataformas que soportan la distribución de contenido protegido por DRM al EU incluyen alguna forma de componente DRM lógico para proporcionar la funcionalidad DRM necesaria en el dominio de plataforma para procesar el contenido protegido por DRM. Por ejemplo, la plataforma para un sistema de telecomunicaciones debe proporcionar un componente DRM lógico para procesar el contenido protegido por DRM que se hace disponible para su descarga a terminales móviles en el sistema. En general, el componente DRM dentro de la plataforma debe proporcionar un soporte de funcionalidad DRM dentro de la plataforma a una aplicación exterior (en el dominio de aplicación) que está proporcionando el contenido a un EU soportado por la plataforma.

El término plataforma, tal como se usa en la presente memoria, se refiere generalmente a una plataforma de software y hardware que conforma, al menos parcialmente, una red "segura" en la que se comunican los usuarios, a través de los EUs, de manera inalámbrica o por cable, o una combinación de los dos. Las entidades de red en la plataforma pueden estar interconectadas a aplicaciones exteriores en el dominio de aplicación con el propósito de descargar contenido protegido por DRM, entre otras cosas. La red se considera segura en el sentido de que la plataforma de red y su tráfico de comunicaciones son gestionados y controlados por un proveedor de red.

Un ejemplo de dicha una red segura es un sistema de telecomunicaciones que comprende, generalmente, EUs (por ejemplo, terminales móviles) que se comunican, de manera inalámbrica, con estaciones base, que a su vez, se comunican con otras entidades de la red de telecomunicaciones y similares. Incluida entre estas otras entidades, hay una interfaz a redes externas, tales como Internet, y aplicaciones externas. Estas aplicaciones exteriores son accesibles a los usuarios dentro de la red a través de las diversas entidades de red y el software que usan para comunicarse y mover datos desde y hacia el usuario (es decir, el software de plataforma) bajo el control del proveedor de la red.

Se emplea un algoritmo de cifrado/descifrado para cifrar y descifrar el contenido. Preferiblemente, el algoritmo es simétrico, lo que significa que se usa una clave idéntica para ambas operaciones, por razones de eficiencia. Sin embargo, las propias claves pueden ser protegidas también usando algoritmos de cifrado asimétricos, que hacen uso de un par de claves pública/privada, según se divulga en la solicitud de patente US2002094084. También se puede obtener una seguridad adicional incorporando el uso de certificados y firmas digitales, tal como se conoce en la técnica. El modelo completo para la distribución segura de claves públicas mediante el uso de certificados y firmas digitales se conoce como la Infraestructura de Clave Pública (Public Key Infrastructure, PKI).

El EU descifra el contenido usando una clave de descifrado suministrada en el objeto de derechos a través de la plataforma. Frecuentemente, se da el caso en el que deben distribuirse claves únicas para descifrar el contenido a cada uno de entre un gran número de EUs. Típicamente, la distribución de un gran número de claves requiere una cantidad de tiempo relativamente importante, lo que fuerza a que la distribución de claves tenga lugar mucho antes de que el contenido se haga disponible, por ejemplo, un evento de transmisión de vídeo/audio planificado, ya que cada clave distribuida es única para cada EU y, típicamente, la distribución sigue protocolos bastante complejos especificados por la solución DRM. El hecho de que la clave o el material de clave estará disponible en el EU mucho tiempo antes de su uso previsto resulta en un mayor riesgo de que la clave se vea comprometida por usuarios no autorizados y quizás incluso sea distribuida ampliamente a otros usuarios no autorizados. Por lo tanto, debería minimizarse el tiempo que la clave (o el material de clave) está presente en el EU antes de su uso previsto. Este problema se agrava cuando la cantidad de ancho de banda disponible para la distribución de claves disminuye, ya que la cantidad de tiempo necesario para distribuir las claves aumenta. Los sistemas, tales como los sistemas de comunicaciones móviles, son especialmente vulnerables, debido a su ancho de banda limitado. Otros dominios, tales como el dominio de radiodifusión digital (TV), tienen suficiente ancho de banda para distribuir la clave sólo poco antes del inicio de una sesión de transmisión de contenido.

COMPENDIO

Se describe un procedimiento para la gestión de derechos digitales en un sistema que incluye un dispositivo, un emisor de contenidos y un emisor de derechos. Una clave de cifrado de contenido (Content Encryption Key, CEK) es cifrada usando una clave pública asociada con el dispositivo para producir una CEK cifrada. La CEK cifrada es cifrada usando una clave de cifrado del emisor que incluye datos correspondientes al emisor de contenidos para producir una CEK cifrada dos veces. La CEK cifrada dos veces es cifrada usando la clave pública asociada con el dispositivo para producir un texto cifrado del objeto de derechos. El texto cifrado del objeto de derechos está disponible para el dispositivo en un punto en el tiempo, y la clave de descifrado del emisor está disponible para el dispositivo en otro punto en el tiempo, siendo ambas claves necesarias para descifrar el contenido digital asociado con el emisor de contenidos.

Un procedimiento para la gestión de derechos digitales en un dispositivo incluye descifrar un texto cifrado del objeto de derechos recibido de un emisor de derechos usando una clave privada asociada con el dispositivo para producir un texto cifrado del objeto de derechos descifrado y descifrar el texto cifrado del objeto de derechos descifrado usando una clave de descifrado del emisor recibida desde un emisor de contenidos para producir una CEK cifrada. La CEK cifrada es descifrada usando la clave privada asociada con el dispositivo para obtener una CEK. A continuación, la CEK está disponible para descifrar el contenido digital asociado con el emisor de contenidos. El texto cifrado del objeto de derechos está disponible para el dispositivo en un punto en el tiempo y la clave de descifrado del emisor está disponible para el dispositivo en otro punto en el tiempo, siendo ambas claves necesarias para descifrar el contenido digital asociado con el emisor de contenidos.

Un sistema para la gestión de derechos digitales que incluye un dispositivo, un emisor de contenidos y un emisor de derechos, incluye una lógica que cifra una clave de cifrado de contenido (CEK) usando una clave pública asociada con un dispositivo para producir una CEK cifrada y una lógica que cifra la CEK cifrada usando una clave de cifrado del emisor que incluye datos correspondientes a un emisor de contenidos para producir una CEK cifrada dos veces. El sistema incluye también una lógica que cifra la CEK cifrada dos veces usando la clave pública asociada con el dispositivo para producir un texto cifrado del objeto de derechos. El texto cifrado del objeto de derechos está disponible para el dispositivo de descifrar el contenido digital asociado con el emisor de contenidos en un punto en el tiempo y la clave de descifrado del emisor está disponible para el dispositivo en otro punto en el tiempo, siendo ambas claves necesarias para descifrar el contenido digital asociado con el emisor de contenidos.

Un aparato para la gestión de derechos digitales incluye lógica que descifra un texto cifrado del objeto de derechos recibido desde un emisor de derechos usando una clave privada asociada con el aparato para producir un texto cifrado del objeto de derechos descifrado y una lógica que descifra el texto cifrado del objeto de derechos descifrado usando una clave de descifrado del emisor recibida desde un emisor de contenidos para producir una CEK cifrada. El aparato incluye también una lógica que descifra la CEK cifrada usando la clave privada asociada con el aparato para obtener una CEK. A continuación, la CEK está disponible para descifrar el contenido digital asociado con el emisor de contenidos. El texto cifrado del objeto de derechos está disponible para el dispositivo en un punto en el tiempo y la clave de descifrado del emisor está disponible para el dispositivo en otro punto en el tiempo, siendo ambas claves necesarias para descifrar el contenido digital asociado con el emisor de contenidos.

BREVE DESCRIPCIÓN DE LOS DIBUJOS

Los objetos y ventajas de la presente invención serán evidentes para las personas con conocimientos en la materia tras la lectura de la presente descripción en conjunción con los dibujos adjuntos, en los que se han usado números de referencia similares para designar elementos similares, y en los que:

La Figura 1 es un diagrama de bloques que ilustra un modelo básico para proporcionar contenido usando DRM.
La Figura 2 es un diagrama de bloques que ilustra el suministro de contenidos usando DRM según un aspecto.
La Figura 3 es un diagrama de bloques que ilustra un dispositivo con capacidad DRM según otro aspecto.
La Figura 4 es un diagrama de flujo que ilustra un procedimiento para DRM según otro aspecto.
La Figura 5 es un diagrama de flujo que ilustra un procedimiento para DRM en un dispositivo según otro aspecto.
La Figura 6 ilustra el cifrado/descifrado de la CEK.

DESCRIPCIÓN DETALLADA

Para facilitar una comprensión de las realizaciones ejemplares, muchos aspectos se describen en términos de secuencias de acciones que pueden ser realizadas por elementos de un sistema informático. Por ejemplo, se reconocerá que en cada una de las realizaciones, las diversas acciones pueden ser realizadas por circuitos o circuitería especializados (por ejemplo, puertas lógicas discretas interconectadas para realizar una función especializada), por instrucciones de programa ejecutadas por uno o más procesadores, o por una combinación de ambos.

Además, las secuencias de acciones pueden ser materializadas en cualquier medio legible por ordenador para su uso por, o en conexión con, un sistema, aparato o dispositivo de ejecución de instrucciones, tal como un sistema basado en

ordenador, un sistema que contiene un procesador u otro sistema que puede recuperar las instrucciones desde un medio legible por ordenador y ejecutar las instrucciones.

Tal como se usa en la presente memoria, un "medio legible por ordenador" puede ser cualquier medio que puede contener, almacenar, comunicar, propagar o transportar el programa para su uso por, o en conexión con, el sistema, aparato o dispositivo de ejecución de instrucciones. El medio legible por ordenador puede ser, por ejemplo, pero sin limitarse a, un sistema aparato, dispositivo o medio de propagación electrónico, magnético, óptico, electromagnético, infrarrojo o semiconductor. Los ejemplos más específicos (una lista no exhaustiva) del medio legible por ordenador pueden incluir los siguientes: una conexión eléctrica que tiene uno o más cables, un disquete de ordenador portátil, una memoria de acceso aleatorio (RAM), una memoria de sólo lectura (ROM), una memoria de sólo lectura programable y borrable (EPROM o memoria Flash), una fibra óptica y un disco compacto portátil memoria de sólo lectura (CD-ROM).

La especificación DRM OMA, V2, propone que un emisor de derechos, es decir, una entidad que emite objetos de derechos, transmita un objeto de derechos que contiene una clave de cifrado de contenidos ("CEK") a un EU (en adelante, el término "dispositivo" se usa en lugar de EU para corresponderse con la terminología DRM OMA) que es cifrada con la clave pública del dispositivo. De manera más precisa, la clave de cifrado de contenidos es cifrada junto con los derechos (y otra información sensible del objeto de derechos) usando una clave de cifrado de objeto de derechos, y la clave de cifrado de objeto de derechos es cifrada junto con una clave MAC (para la protección de la integridad del objeto de derechos) usando la clave pública del dispositivo, y el texto cifrado resultante es incluido en el objeto de derechos. En aras de la simplicidad, en la presente memoria, estas operaciones se remplazan por una operación de cifrado. A continuación, un agente de DRM en el dispositivo usa la clave privada del dispositivo para descifrar el objeto de derechos para obtener la CEK que, a continuación, puede ser usada para descifrar el contenido de la transmisión. Sin embargo, este enfoque resulta en un mayor riesgo de que la CEK se vea comprometida por usuarios no autorizados y/o sea distribuida a otros usuarios no autorizados. Es decir, la clave puede ser pirateada antes de la sesión de transmisión continua (por ejemplo, debido a una mala implementación de DRM en el dispositivo), y la CEK comprometida puede ser distribuida a un gran número de usuarios (por ejemplo, a través de Internet) que, a continuación, pueden usarla para descifrar el contenido de la transmisión continua.

La Figura 2 es un diagrama de bloques que ilustra el suministro de contenido usando DRM para un caso de uso de contenido de transmisión continua. Hay cuatro agentes, un emisor 200 de contenidos, un emisor 210 de derechos, un EU 250 y un servidor 220 de transmisión continua. El emisor 200 de contenidos, el emisor 210 de derechos y el servidor 220 de transmisión continua se muestran, de manera lógica, como entidades separadas, pero se apreciará que estos agentes pueden combinarse física y/o lógicamente. Aquí, el término agente se refiere a un componente de software o una rutina que realiza una acción cuando se produce un evento especificado. Las instrucciones del agente se ejecutan a través de un sistema, aparato o dispositivo de ejecución de instrucciones, tal como un sistema basado en ordenador, un sistema que contiene un procesador u otro sistema que puede recuperar instrucciones y ejecutar las instrucciones.

El emisor 210 de derechos reenvía un objeto de 260 derechos al dispositivo 250 que contiene los derechos, es decir, permisos y restricciones que definen las circunstancias bajo las cuales se concede el acceso a los contenidos DRM, y un texto 261 cifrado de objeto de derechos que es la forma cifrada de la CEK necesaria para descifrar el contenido DRM según los derechos. El emisor 200 de contenidos reenvía una clave 270 de descifrado del emisor (Issuer Decryption Key, "IDK") al dispositivo para su uso en la obtención de la CEK (para descifrar el contenido) a partir del texto 261 cifrado del objeto de derechos. Usando esta técnica, el objeto 260 de derechos puede ser proporcionado con suficiente antelación al contenido. Sin embargo, la CEK no puede ser obtenida hasta que la IDK 270 es recibida en el dispositivo 250. La IDK 270 no es específica del dispositivo (puede ser la misma para todos los dispositivos) y, por lo tanto, puede ser difundida a todos los dispositivos que reciben ese contenido particular justo antes de enviar el contenido. En consecuencia, la CEK sólo puede ser descifrada completamente por el dispositivo 250, es decir, puede ser usada en el dispositivo 250, poco antes de que el contenido sea recibido, lo que minimiza el tiempo para piratear la CEK en busca de un uso no autorizado. Además, el texto 261 cifrado del objeto de derechos puede ser distribuido a cada dispositivo con mucha antelación, incluso en sistemas que tienen un ancho de banda limitado para este propósito, tal como un sistema de telecomunicaciones. Una vez obtenida la CEK, el contenido 280 cifrado con CEK que es recibido por el dispositivo 250 desde el servidor 220 de transmisión continua puede ser descifrado y el contenido puede ser reproducido por el dispositivo 250.

La Figura 4 es un diagrama de flujo que ilustra un procedimiento para DRM según otro aspecto. La CEK es cifrada (400) usando una clave pública ("DPuK") asociada con el dispositivo 250 para producir una CEK cifrada (CEK"). La CEK cifrada (CEK") es cifrada (410) de nuevo usando una clave de cifrado del emisor que incluye datos correspondientes al emisor de contenidos para producir una CEK cifrada dos veces (CEK'). Aquí, la CEK cifrada puede ser cifrada junto con los derechos y otra "información sensible". Dicha información sensible podría incluir cualquier otro dato que podría beneficiarse de la integridad y/o protección de la confidencialidad añadidas, tal como una clave para la protección de la integridad del objeto de derechos. La CEK cifrada dos veces (CEK') es cifrada (420) usando la DPuK para producir el texto 261 cifrado del

objeto de derechos, que está disponible para el dispositivo 250 para descifrar el contenido 280 digital asociado con el emisor 200 de contenidos.

El procedimiento es realizado por el emisor 210 de derechos solo o en cooperación con el emisor 200 de contenidos. El emisor 210 de derechos compila el conocimiento de la CEK, la clave 270 de cifrado del emisor ("IEK") y la DPuK específica del dispositivo. La Figura 6 ilustra el cifrado de la CEK 600. La DPuK es aplicada para cifrar la CEK 600 y producir la CEK" 610, es decir, CEK" = E_{DPuK} (CEK). En esta etapa, se podría usar el algoritmo RSA. La IEK es aplicada para cifrar la CEK" 610 y producir la CEK' 620, es decir, CEK' = E_{IEK} (CEK"). Aquí, el cifrado es realizado, preferiblemente, usando un cifrado simétrico, tal como el estándar de cifrado avanzado (Advance Encryption Standard, "AES"). Pueden emplearse también otros procedimientos de cifrado simétrico o asimétrico. Si se usa un cifrado simétrico, entonces la clave de cifrado del emisor es igual a la clave de descifrado del emisor, es decir, IEK = IDK. La DPuK es aplicada para cifrar la CEK' 620 y producir el texto 630 cifrado del objeto de derechos ("ROC"), es decir, ROC = E_{DPuK} (CEK'). También, en esta etapa, se podría usar el algoritmo RSA, y esta etapa podría implicar una o más transformaciones tales como, por ejemplo, en DRM OMA V2, indicada anteriormente.

Con referencia de nuevo a la Figura 2, una vez producido el texto 261cifrado del objeto de derechos, es reenviado con el objeto 260 de derechos al dispositivo 250 por el emisor 210 de derechos. Este puede ser reenviado con suficiente antelación al contenido 280 cifrado con CEK, ya que el dispositivo 250 no será capaz de descifrar la CEK' 620 hasta que no se reciba la IDK 270 desde el emisor 200 de contenidos. Debido a que la CEK' 620 es un dispositivo único y la clave privada de dispositivo es necesaria para obtener la CEK, un hacker debe publicar tanto la CEK' como su clave privada a través de, por ejemplo, Internet, para permitir que otras personas sean capaces de obtener la CEK cuando la IDK es difundida. Sin embargo, probablemente, la publicación de su clave privada no es algo que el hacker quiera hacer. La clave privada del dispositivo sólo es accesible por el agente DRM del dispositivo. Los usuarios del EU u otras personas no tienen acceso a esta clave.

La Figura 3 es un diagrama de bloques que ilustra un dispositivo con capacidad DRM. Un receptor 300 recibe señales de manera inalámbrica a través de una antena 340 o a través de otro medio conocido en la técnica, tal como un cable, un cable de fibra óptica, etc. El receptor 300 convierte las señales recibidas a un formato que es reconocido por un procesador 310 para procesar las señales. El procesador 310 accede a una memoria 320, tal como RAM, ROM, etc., para recuperar instrucciones y/o información almacenada. Por ejemplo, las instrucciones que forman un algoritmo de descifrado y/o claves de descifrado pueden estar almacenadas en la memoria 320 y pueden ser recuperadas por el procesador 310 para descifrar el contenido recibido a través del receptor 300. Una vez que el contenido ha sido descifrado por el procesador 310, el contenido puede ser sometido a transformaciones adicionales, tales como descompresión y, a continuación, es reenviado a algunos medios 330 de salida asociados con el dispositivo, tales como una o más pantallas y/o altavoces.

La Figura 5 es un diagrama de flujo que ilustra un procedimiento de DRM en un dispositivo. El texto 261 cifrado del objeto de derechos recibido desde el emisor 210 de derechos es descifrado (500) usando una clave 251 privada ("DPrK") asociada con el dispositivo para producir un texto cifrado del objeto de derechos descifrado. La DPrK 251 del dispositivo está sólo accesible para el agente de DRM del dispositivo. Los usuarios del EU u otras personas no tienen acceso a esta clave. La CEK' descifrada es descifrada (510) usando la IDK 270 recibida del emisor 200 de contenidos para producir una CEK cifrada. La CEK cifrada es descifrada (520) usando la DPrK 251 para obtener la CEK. A continuación, la CEK está disponible para descifrar el contenido digital asociado con el emisor 200 de contenidos. En la etapa 420 de la Figura 4, la CEK es cifrada una vez más con la clave DPuK pública del dispositivo como en la etapa 400 de la Figura 4, lo que podría parecer innecesario. Sin embargo, la etapa 420 en la Figura 4 (y la etapa 500 en la Figura 5) corresponde al cifrado de la CEK tal como se describe en DRM OMA V2, descrita anteriormente (o un esquema similar), y no sólo implica el cifrado de la CEK, sino que también se cifra otra información sensible del objeto de derechos. Este cifrado incluye también una clave MAC usada para proteger la integridad del objeto de derechos que incluye la CEK cifrada dos veces y los derechos. En cuanto el dispositivo DRM recibe el objeto de derechos desde el emisor de derechos, el texto cifrado del objeto de derechos puede ser descifrado para comprobar la integridad del objeto de derechos, obtener la CEK', los derechos y otros datos sensibles desde el objeto de derechos, etc. Sin embargo, la CEK no puede ser obtenida hasta que llegue la IDK 270.

La Figura 6 ilustra también el descifrado de un texto 630 cifrado del objeto de derechos en el dispositivo 250, usando la DPrK 251 en el dispositivo 250, por ejemplo, a través de un agente DRM asociado con el dispositivo 250. El texto 630 cifrado del objeto de derechos es descifrado usando la DPrK 251 para producir la CEK' 620, es decir, CEK' = D_{DPrK} (ROC). Esto podría implicar una o más transformaciones. La CEK' 620 es descifrada usando la IDK 270 para producir la CEK" 610, es decir, CEK" = D_{IDK} (CEK'). Aquí, el descifrado es realizado, preferiblemente, usando un cifrado simétrico, tal como AES. Pueden emplearse también otros procedimientos simétricos o asimétricos de cifrado/descifrado. La CEK" 610 es descifrada usando la DPrK 251 para producir la CEK 600, es decir, CEK = D_{DPrK} (CEK").

Tal como se puede apreciar, las etapas ilustradas por la Figura 5 son inversas a las etapas ilustradas en la Figura 4, y

puede emplearse cualquier nivel de simetría, de manera que uno o más de los sistemas de cifrado en una operación tengan que ser usados también en la operación opuesta respectiva.

Una vez producida la CEK en el dispositivo 250, el contenido digital, es decir, el contenido 280 cifrado con CEK, asociado con el emisor 200 de contenidos, puede ser recibido desde el servidor 220 de transmisión continua y puede ser descifrado usando la CEK 600.

Debido a que la IDK 270 no es específica del dispositivo, la misma IDK 270 puede ser reenviada a una pluralidad de dispositivos. En consecuencia, la IDK 270 puede ser "difundida" a todos los dispositivos que reciben el contenido en un tiempo relativamente corto incluso usando un ancho de banda limitado, tal como está disponible en un sistema de telecomunicaciones. Por consiguiente, la IDK 270 puede ser reenviada a, y recibida en el dispositivo 250 como una parte inicial del contenido 280 digital o justo antes de que el dispositivo 250 reciba el contenido 200 digital. Por ejemplo, la IDK 270 podría ser seleccionada de manera que sea también el valor inicial usado en el cifrado del contenido 200 digital.

Opcionalmente, la IDK 270 también puede ser firmada digitalmente antes de ser reenviada al dispositivo 250. Por ejemplo, el emisor 200 de contenidos o el emisor 210 de derechos pueden firmar digitalmente la IDK 270 usando una clave privada para garantizar que la IDK 270 no es modificada durante la transmisión al dispositivo 250. El agente de DRM en el dispositivo 250 verifica la firma usando la clave pública correspondiente, la cual puede hacerse disponible para el dispositivo 250. En DRM OMA V2, la clave pública del emisor de derechos es suministrada ya al dispositivo durante la fase de registro del emisor de derechos y se usa para autenticar el emisor 210 de derechos. En consecuencia, el par de claves del emisor de derechos puede ser usado para firmar la IDK 270 con un mínimo impacto sobre la infraestructura DRM OMA V2 actual.

Los procedimientos, sistemas y aparatos descritos por el presente solicitante reducen, de manera significativa, el riesgo de uso no autorizado debido al hackeado de la CEK. Además, hay un beneficio añadido de mejorar la escalabilidad a un gran número de dispositivos 250.

La IDK 270 puede ser reenviada junto con otros datos usados para otros propósitos en el dispositivo 250. Siempre que los otros datos no sean específicos del dispositivo, se mantendrán los beneficios de escalabilidad y difusión. El dispositivo 250 simplemente extraería la IDK 270 del otro dato antes de usarlo.

Debería apreciarse que el término "clave", tal como se usa en la descripción y en las reivindicaciones, incluye no solo las claves de cifrado/descifrado, sino también datos o información que pueden ser usados para generar una o más claves de cifrado/descifrado. Para aumentar adicionalmente la seguridad contra la amenaza de que la CEK sea publicada en Internet por un hacker en el momento en el que se inicia la sesión de transmisión continua y que un usuario pudiera obtener la CEK y, entonces, solo se pierda la primera parte del contenido transmitido, la clave de cifrado de contenido podría ser cambiada (actualización de clave) durante la sesión de transmisión continua. A continuación, el esquema es extendido para abarcar un conjunto de claves de cifrado de contenido {CEK1, CEK2, ..., CEKn} y un conjunto de claves de cifrado del emisor (IEK1, IEK2, ..., IEKn). Cada CEKi es cifrada usando la clave pública del dispositivo para generar' CEKi". A continuación, cada CEKi" es cifrada con diferentes claves de cifrado del emisor IEKi en CEKi". A continuación, CEK1', ..., CEKn' son concatenadas y cifradas e incluidas en el RO usando el mismo cifrado que el usado para una única CEK', tal como se ha descrito anteriormente. Cuando el RO es obtenido por el dispositivo de DRM, el texto cifrado de RO puede ser descifrado para obtener CEK1', ..., CEKn'. Las claves de descifrado del emisor (IDK1, ..., IDKn) serán enviadas periódicamente justo antes de cambiar las claves de cifrado de contenido durante la transmisión, de manera que cuando IDKi es obtenida el agente DRM puede calcular CEKi, tal como se ha descrito anteriormente.

Las personas con conocimientos ordinarios en la materia apreciarán que la invención puede ser materializada en diversas formas específicas sin apartarse de sus características esenciales. Las realizaciones descritas se consideran en todos los aspectos como ilustrativas y no restrictivas. El alcance de la invención viene indicado por las reivindicaciones adjuntas, en lugar de por la descripción anterior, y todos los cambios incluidos dentro del significado y el rango de equivalentes de las mismas están destinados a estar incluidos en la misma.

Debería enfatizarse que los términos "comprende" y "que comprende", cuando se usan en la presente descripción y en las reivindicaciones, se entiende que especifican la presencia de características, etapas o componentes indicados, pero el uso de estos términos no excluye la presencia o adición de una o más de entre otras características, etapas, componentes o grupos de los mismos.

REIVINDICACIONES

1. En un sistema que soporta la gestión de derechos digitales y que incluye un dispositivo, un emisor de contenidos y un emisor de derechos, un procedimiento para la gestión de derechos digitales que comprende:

cifrar (400) una clave de cifrado de contenidos CEK (600) usando una clave pública asociada con el dispositivo para producir una CEK (610) cifrada;
cifrar (410) la CEK cifrada usando una clave de cifrado del emisor que incluye datos correspondientes al emisor de contenidos para producir una CEK (620) cifrada dos veces, y
cifrar (420) la CEK cifrada dos veces usando la clave pública asociada con el dispositivo para producir un texto (630) cifrado de objeto de derechos, estando el texto cifrado del objeto de derechos disponible para el dispositivo en un punto en el tiempo, y estando disponible la clave de descifrado del emisor para el dispositivo en otro punto en el tiempo, siendo ambas claves necesarias para descifrar el contenido digital asociado con el emisor de contenidos.

2. Procedimiento según la reivindicación 1, que comprende:

reenviar, por el emisor de derechos, el texto cifrado del objeto de derechos al dispositivo.

3. Procedimiento según la reivindicación 2, que comprende:

reenviar, por el emisor de contenidos, la clave de cifrado del emisor al dispositivo.

4. Procedimiento según la reivindicación 1, que comprende:

cifrar la CEK cifrada junto con una clave para la protección de la integridad del objeto de derechos.

5. Procedimiento según la reivindicación 3, que comprende:

en el dispositivo:
descifrar el texto cifrado del objeto de derechos usando una clave privada asociada con el dispositivo para producir un texto cifrado del objeto de derechos descifrado;
descifrar el texto cifrado del objeto de derechos descifrado usando una clave de descifrado del emisor recibida desde el emisor de contenidos para producir una CEK cifrada, y
descifrar la CEK cifrada usando la clave privada asociada con el dispositivo para obtener una CEK, estando disponible la CEK para descifrar el contenido digital asociado con el emisor de contenidos.

6. Procedimiento según la reivindicación 5, que comprende:

recibir, en el dispositivo, el contenido digital asociado con el emisor de contenidos, y
descifrar el contenido digital usando la CEK.

7. Procedimiento según la reivindicación 3, en el que la misma clave de descifrado del emisor es reenviada a una pluralidad de dispositivos.

8. Procedimiento según la reivindicación 3, en el que la clave de descifrado del emisor es reenviada al dispositivo como una parte inicial del contenido digital asociado con el emisor de contenidos.

9. Procedimiento según la reivindicación 6, en el que la clave de descifrado del emisor es reenviada al dispositivo justo antes de que el dispositivo reciba el contenido digital asociado con el emisor de contenidos.

10. Procedimiento según la reivindicación 3, en el que la clave de descifrado del emisor es firmada digitalmente antes de ser reenviada al dispositivo.

11. Procedimiento según la reivindicación 5, que comprende:

descifrar la CEK cifrada usando la clave privada asociada con el dispositivo para obtener una CEK y una clave para la protección de la integridad del objeto de derechos.

12. Procedimiento para la gestión de derechos digitales en un dispositivo, que comprende:

descifrar un texto cifrado de un objeto de derechos recibido desde un emisor de derechos usando una clave privada asociada con el dispositivo para producir un texto cifrado del objeto de derechos descifrado;
descifrar el texto cifrado del objeto de derechos descifrado usando una clave de descifrado del emisor recibida desde un emisor de contenidos para producir una CEK cifrada, y
descifrar la CEK cifrada usando la clave privada asociada con el dispositivo para obtener una CEK, estando disponible la CEK para descifrar el contenido digital asociado con el emisor de contenidos
en el que el texto cifrado del objeto de derechos está disponible para el dispositivo en un punto en el tiempo y la clave de descifrado del emisor está disponible para el dispositivo en otro punto en el tiempo, siendo ambas claves necesarias para descifrar el contenido digital asociado con el emisor de contenidos.

13. Procedimiento según la reivindicación 12, que comprende:

recibir contenido digital asociado con el emisor de contenidos, y
descifrar el contenido digital usando la CEK.

14. Procedimiento según la reivindicación 12, en el que la clave de descifrado del emisor es recibida en el dispositivo como una parte inicial del contenido digital asociado con el emisor de contenidos.

15. Procedimiento según la reivindicación 12, en el que la clave de descifrado del emisor es recibida en el dispositivo justo antes de que el dispositivo reciba el contenido digital asociado con el emisor de contenidos.

16. Un sistema para la gestión de derechos digitales que incluye un dispositivo, un emisor de contenidos y un emisor de derechos, comprendiendo el sistema:

lógica que cifra una clave de cifrado de contenido (CEK) usando una clave pública asociada con un dispositivo para producir una CEK cifrada;
lógica que cifra la CEK cifrada usando una clave de cifrado del emisor que incluye datos correspondientes a un emisor de contenidos para producir una CEK cifrada dos veces, y
lógica que cifra la CEK cifrada dos veces usando la clave pública asociada con el dispositivo para producir un texto cifrado del objeto de derechos, estando disponible el texto cifrado del objeto de derechos para el dispositivo en un punto en el tiempo, y estando disponible la clave de descifrado del emisor para el dispositivo en otro punto en el tiempo, siendo ambas necesarias para descifrar el contenido digital asociado con el emisor de contenidos.

17. Sistema según la reivindicación 16, que comprende:

lógica que reenvía, desde un emisor de derechos, el objeto de derechos al dispositivo.

18. Sistema según la reivindicación 17, que comprende:

lógica que reenvía, desde el emisor de contenidos, la clave de cifrado del emisor al dispositivo.

19. Sistema según la reivindicación 16, que comprende:

lógica que cifra la CEK cifrada junto con una clave de protección de la integridad del objeto de derechos.

20. Sistema según la reivindicación 18, en el que el dispositivo comprende:

lógica que descifra el texto cifrado del objeto de derechos usando una clave privada asociada con el dispositivo para producir un texto cifrado del objeto de derechos descifrado;
lógica que descifra el texto cifrado del objeto de derechos descifrado usando la clave de descifrado del emisor para producir una CEK cifrada, y
lógica que descifra la CEK cifrada usando la clave privada asociada con el dispositivo para obtener una CEK, estando disponible la CEK para descifrar el contenido digital asociado con el emisor de contenidos.

21. Sistema según la reivindicación 20, en el que el dispositivo incluye:

lógica que recibe el contenido digital asociado con el emisor de contenidos, y
lógica que descifra el contenido digital usando la CEK.

22. Sistema según la reivindicación 18, en el que el dispositivo incluye una lógica que reenvía la misma clave de

descifrado del emisor a una pluralidad de dispositivos.

23. Sistema según la reivindicación 18, en el que el dispositivo incluye lógica que reenvía la clave de descifrado del emisor al dispositivo como una parte inicial del contenido digital asociado con el emisor de contenidos.

24. Sistema según la reivindicación 18, en el que el dispositivo incluye una lógica que reenvía la clave de descifrado del emisor al dispositivo justo antes de que el dispositivo reciba el contenido digital asociado con el emisor de contenidos.

25. Sistema según la reivindicación 18, en el que el dispositivo incluye una lógica que firma digitalmente la clave de descifrado del emisor antes de reenviarla.

26. Sistema según la reivindicación 20, que comprende:

lógica que descifra la CEK cifrada usando la clave privada asociada con el dispositivo para obtener una CEK y una clave para la protección de la integridad del objeto de derechos.

27. Un aparato para la gestión de derechos digitales, que comprende:

lógica que descifra un texto cifrado del objeto de derechos recibido desde un emisor de derechos usando una clave privada asociada con el aparato para producir un texto cifrado del objeto de derechos descifrado;
lógica que descifra el texto cifrado del objeto de derechos descifrado usando una clave de descifrado del emisor recibida desde un emisor de contenidos para producir una CEK cifrada, y
lógica que descifra la CEK cifrada usando la clave privada asociada con el aparato para obtener una CEK, estando disponible la CEK para descifrar el contenido digital asociado con el emisor de contenidos
en el que el texto cifrado del objeto de derechos está disponible para el dispositivo en un punto en el tiempo y la clave de descifrado del emisor está disponible para el dispositivo en otro punto en el tiempo, siendo ambas claves necesarias para descifrar el contenido digital asociado con el emisor de contenidos.

28. Aparato según la reivindicación 27, que comprende:

lógica que recibe el contenido digital asociado con el emisor de contenidos, y
lógica que descifra el contenido digital usando la CEK.

29. Aparato según la reivindicación 27, en el que la clave de descifrado del emisor es recibida y procesada por el aparato como una parte inicial del contenido digital asociado con el emisor de contenidos.

30. Aparato según la reivindicación 27, en el que la clave de descifrado del emisor es recibida y procesada por el aparato justo antes de que el aparato reciba el contenido digital asociado con el emisor de contenidos.

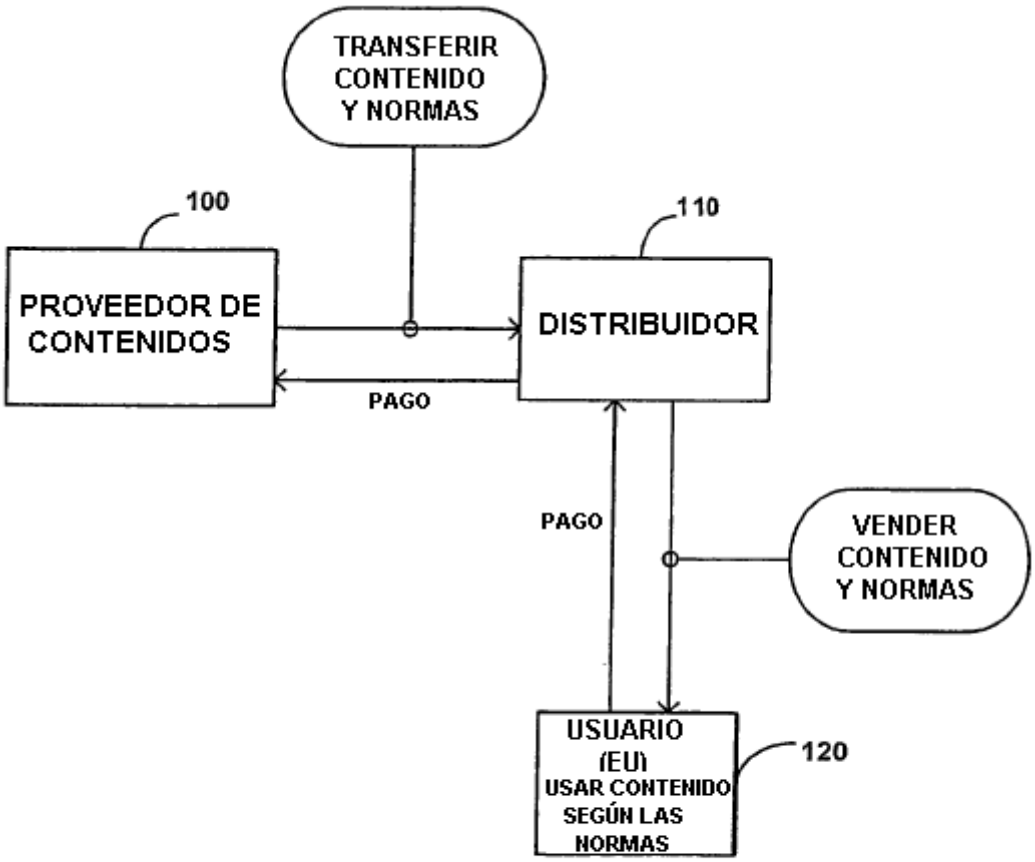
TRANSFERIR CONTENIDO Y NORMAS
100
110
PROVEEDOR DE CONTENIDOS
DISTRIBUIDOR
PAGO
PAGO
VENDER CONTENIDO Y NORMAS
USUARIO (EU) USAR CONTENIDO SEGÚN LAS NORMAS
120

FIG. 1

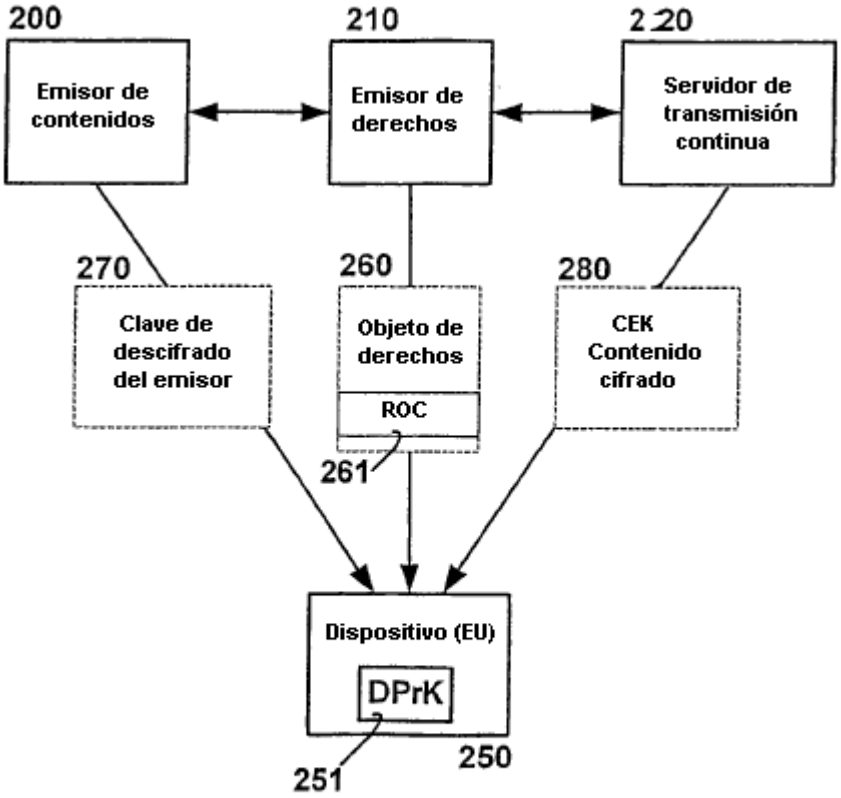
200
Emisor de contenidos
210
Emisor de derechos
220
Servidor de transmisión continua
270
Clave de descifrado del emisor
260
Objeto de derechos
ROC
261
280
CEK Contenido cifrado
Dispositivo (EU)
DPrK
251
250

FIG. 2

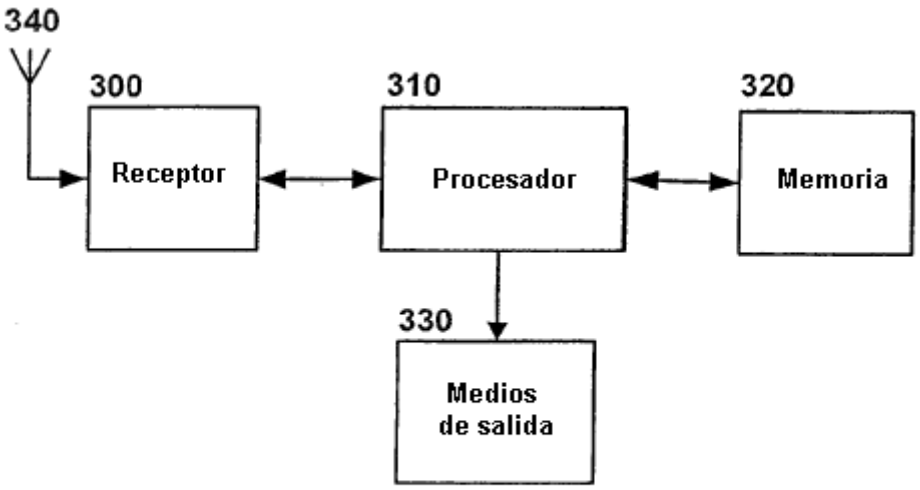
340
300
Receptor
310
Procesador
320
Memoria
330
Medios
de salida

FIG 3

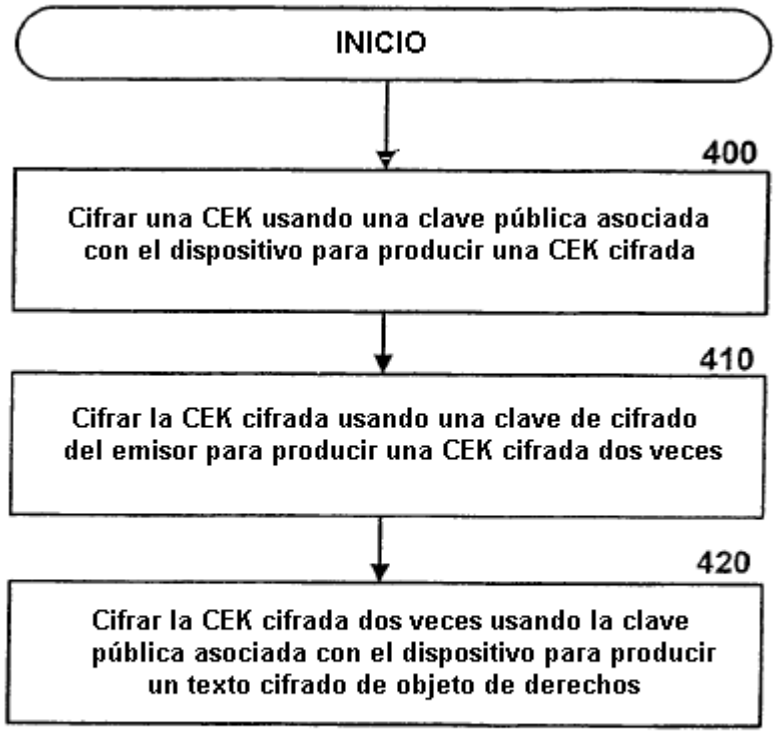
INICIO
400
Cifrar una CEK usando una clave pública asociada con el dispositivo para producir una CEK cifrada
410
Cifrar la CEK cifrada usando una clave de cifrado del emisor para producir una CEK cifrada dos veces
420
Cifrar la CEK cifrada dos veces usando la clave pública asociada con el dispositivo para producir un texto cifrado de objeto de derechos

FIG 4

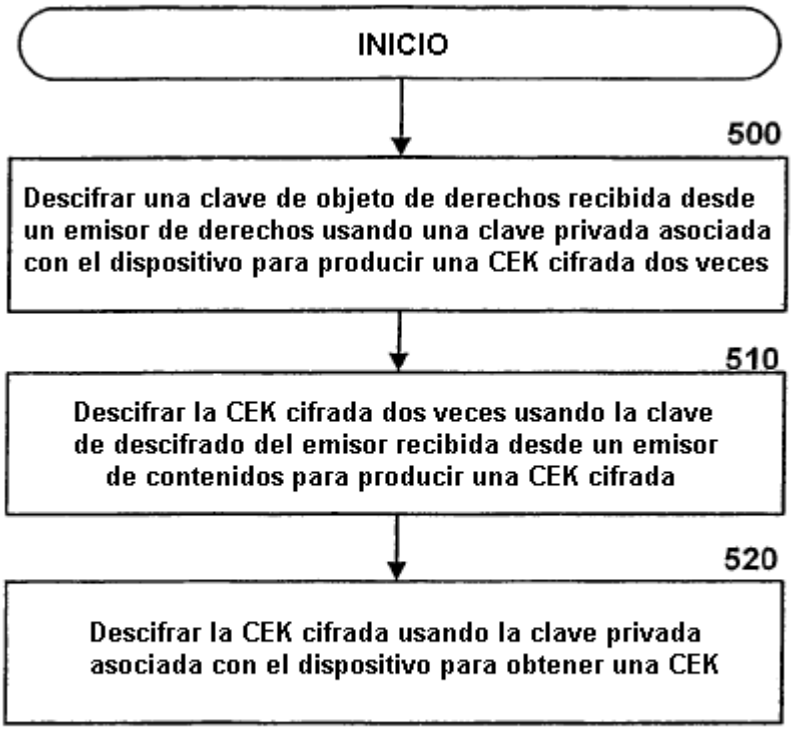
INICIO
500
Descifrar una clave de objeto de derechos recibida desde un emisor de derechos usando una clave privada asociada con el dispositivo para producir una CEK cifrada dos veces
510
Descifrar la CEK cifrada dos veces usando la clave de descifrado del emisor recibida desde un emisor de contenidos para producir una CEK cifrada
520
Descifrar la CEK cifrada usando la clave privada asociada con el dispositivo para obtener una CEK

FIG 5

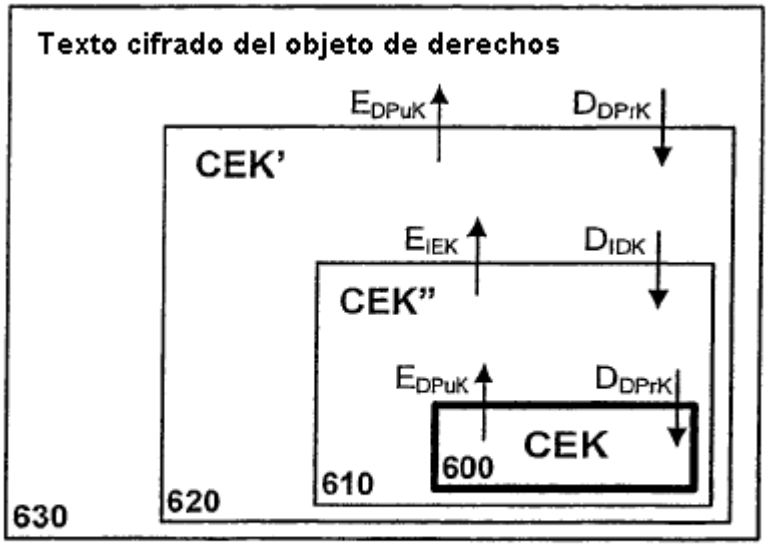
Texto cifrado del objeto de derechos
EDPuK
DDPrK
CEK'
EIEK
DIDK
CEK"
EDPuK
DDPrK
CEK
600
610
620
630

FIG 6