(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 557 439**

(51) Int. CI.:

G11B 20/00 (2006.01)
G06F 21/10 (2013.01)
H04H 20/31 (2008.01)
H04L 29/06 (2006.01)
H04N 5/913 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **16.10.2002 E 02801461 (1)**

(97) Fecha y número de publicación de la concesión europea: **18.11.2015 EP 1444690**

(54) Título: **Sistema y método para copiar y mover contenidos de manera controlada entre dispositivos y dominios sobre la base de una encriptación condicional de clave de contenido en función del estado de uso**

(30) Prioridad:

18.10.2001 US 982573

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
26.01.2016

(73) Titular/es:

NOKIA TECHNOLOGIES OY (100.0%)
Karaportti 3
02610 Espoo, FI

(72) Inventor/es:

ALVE, JUKKA;
CHIU, PETER K.;
YAN, ZHENG y
HIETASARKA, JUHA

(74) Agente/Representante:

VALLEJO LÓPEZ, Juan Pedro

DESCRIPCIÓN

Sistema y método para copiar y mover contenidos de manera controlada entre dispositivos y dominios sobre la base de una encriptación condicional de clave de contenido en función del estado de uso

Antecedentes de la invención

En los últimos años, la cantidad de información disponible en formato digital ha crecido de manera significativa. Los datos digitales, que se reproducen y se distribuyen fácilmente, pero que mantienen una calidad superior, han sido muy beneficiosos para los proveedores de contenidos de información y de medios. Las ventajas para los proveedores de contenidos, sin embargo, no son absolutas. Los mismos factores que hacen los datos digitales atractivos, como su formato de distribución, es decir, alta calidad, reproducción fácil y rápida distribución, se aplican por igual a los piratas que hacen y distribuyen copias sin licencia de los datos. Además, con el acceso a los medios de distribución, como internet, pueden crearse sin esfuerzo millones de copias pirata sin licencia. Este tipo de copia sin licencia ya está muy extendida en la industria musical con los usuarios de servicios de intercambio de archivos peer-to-peer, como Gnutella, y cuesta millones a la industria musical en ingresos potenciales.

En la técnica anterior, existen técnicas de protección de copias para abordar estas cuestiones. Por ejemplo, los contenidos pueden vincularse al dispositivo del usuario encriptando los contenidos con una única clave en el dispositivo. Este enfoque, sin embargo, limita notablemente lo que los usuarios con una licencia válida pueden hacer con sus contenidos. Los consumidores esperan poder tener un poco de libertad en la manera en que usan sus contenidos. Esperan poder transferir los contenidos a otros dispositivos que usan; y esperan poder hacer copias de seguridad para proteger sus contenidos en el caso de un fallo de hardware. Los compradores de música, por ejemplo, esperan poder escuchar la música que compran en casa, en el equipo de música de su coche, y en dispositivos de audio portátiles. En consecuencia, los sistemas excesivamente restrictivos que impiden estos tipos de usos es poco probable que sean aceptados en el mercado.

"SDMI Secure Digital Music Initiative", SDMI Portable Device Specification, parte 1, versión 1.0, PDWG, Los Angeles, 8 de julio de 1999, establece los requisitos de cumplimiento para un sistema en el que el contenido puede encriptarse para su transmisión a un dispositivo que usa una clave privada y cuyo contenido original se vuelve inutilizable después de completarse la transmisión. Además, la referencia se dirige al documento WO 00/08909 A2 y Harney et al: "Group Secure Association Key Management Protocol", marzo de 2001, Sparta Inc. NSA, XP015023928.

Sumario de la invención

La invención se define por las reivindicaciones.

Un método ilustrativo incluye la recepción de un contenido en el dispositivo de un usuario. El contenido recibido se encripta con una clave de contenido. La clave de contenido se protege encriptándola con una clave de dominio. Los dispositivos compatibles de un usuario, o los dispositivos compatibles de una familia, pueden organizarse en un dominio autorizado. Todos los dispositivos en un dominio autorizado tendrían la capacidad de desencriptar la clave de contenido encriptada. Un usuario puede enviar libremente el contenido encriptado y la clave de contenido encriptada a otros dispositivos en el dominio. En el dispositivo de recepción, se desencripta la clave de contenido en su forma legible. La clave de contenido legible está entonces disponible para desencriptar el contenido. Esto garantiza a los proveedores de contenidos que sus contenidos no serán objeto de la piratería generalizada, ya que solo los dispositivos dentro del dominio del usuario pueden desencriptar las claves de contenido encriptadas con la clave de dominio.

Puede garantizarse la compatibilidad con versiones anteriores al permitir que los proveedores de contenidos distingan un contenido protegido de un contenido no protegido o heredado. Esto se lograría aplicando una marca de agua digital al contenido protegido a través del uso de cualquiera de una serie de técnicas conocidas, tales como las proporcionadas por la corporación Digimarc. Las marcas de agua están integradas en el contenido y pueden hacerse para ser perceptibles o imperceptibles a los usuarios. Los dispositivos autorizados pueden eliminar las marcas de agua perceptibles para garantizar que el contenido no se obstruye cuando se reproduce. Las marcas de agua digitales tienen la ventaja de ser robustas, lo que significa que una vez integradas es difícil eliminarlas del contenido, incluso si el contenido se traduce a otros formatos, por ejemplo, si el contenido se imprime o se traduce a un formato analógico.

Cuando se emplean marcas de agua, un dispositivo que recibe el contenido comprueba la marca de agua. El contenido que está marcado con agua se trata como un contenido protegido y se somete a los mecanismos de protección descritos en el presente documento. El contenido que no está marcado con agua se trata como un contenido no protegido. Como tal, no se aplica una encriptación al contenido y la transferencia del contenido a otros dominios será exitosa.

Puede autorizarse a los proveedores de contenidos a incluir información con el contenido que establece las maneras en que los consumidores pueden usar el contenido dentro de su dominio. Por ejemplo, una transmisión de vídeo digital (DVB) podría incluir una información de estado de uso en una tabla de información de servicio (SI) del programa. La información de estado de uso se lee por el dispositivo compatible y le dice cómo el consumidor puede usar el contenido. Por ejemplo, el estado de uso podría permitir que el consumidor moviera el programa de un dispositivo a otro, pero no copiar el programa. O bien, la información de estado de uso podría establecer que no se permita ninguna copia o movimiento.

Cuando se emplean los estados de uso, los dispositivos que reciben el contenido comprueban su estado de uso. Si se aplica cualquier restricción de uso, es decir, el estado de uso no indica el uso como no restringido, se encripta la clave de contenido con una clave de dispositivo. La encriptación con la clave de dispositivo garantiza que solo el dispositivo receptor puede desencriptar la clave de contenido. En consecuencia, el dispositivo receptor tiene la capacidad de comprobar que las restricciones de uso se cumplen antes de que se use el contenido.

En algunas realizaciones, las marcas de agua y los estados de uso pueden aplicarse conjuntamente para proporcionar una seguridad adicional. En tal realización, puede incorporarse un ID de contenido en la marca de agua. El mismo ID de contenido también está asociado al estado de uso, por lo que el contenido marcado con agua solo se vincula al estado de uso específico. Este enfoque tiene la ventaja de garantizar que el sistema no puede eludirse por los intentos de asociar diferentes estados de uso, menos restrictivos, con el contenido marcado con agua.

En algunas realizaciones de la invención, puede permitirse una mayor libertad para los usuarios regulando la forma de usar el contenido fuera del dominio autorizado. Puede incluirse un indicador de desplazamiento de dominio con el contenido de la misma manera desvelada para el estado de uso. El indicador de desplazamiento de dominio indica si se permite la transferencia del contenido fuera del dominio. Puede usarse una combinación del estado de uso y el indicador de desplazamiento de dominio para establecer con precisión lo que puede hacerse con el contenido dentro y fuera del dominio.

Tales métodos pueden configurarse para permitir que el proveedor de contenidos, o el proveedor de servicios de protección de contenidos, sepan qué clave de contenido debe usarse para encriptar el contenido sin transmitir la propia clave. El proveedor de contenidos puede disponerse para transmitir un valor inicial de clave de contenido con el contenido. A continuación, se genera la clave de contenido en el dispositivo receptor operando sobre el valor inicial de clave de contenido con la clave de dominio del dispositivo, de la que el proveedor de contenidos tiene una copia. El proveedor de contenidos puede restablecer la clave de contenido, si fuera necesario, usando su copia de la misma clave de dominio para operar sobre el valor inicial de clave de contenido de la misma manera.

Gracias a la presente invención son posibles una multitud de interacciones y de relaciones comerciales. Cuando la presente invención se usa para transacciones complejas entre los usuarios, proveedores de contenidos, creadores de contenidos, etc., puede emplearse un proveedor de gestión de confianza. El proveedor de gestión de confianza puede alinear diferentes infraestructuras de confianza usadas en diferentes dispositivos autorizados, facilitar la transferencia de contenidos entre los usuarios de diferentes proveedores de contenidos, o actuar como intermediario para apoyar nuevos modelos de negocio. Esto se logra proporcionando un tercero de confianza neutral que puede cumplir los requisitos del sistema de protección de contenidos.

A continuación, se describirán ejemplos de las realizaciones de la invención con referencia a los dibujos adjuntos.

Breve descripción de las figuras

La figura 1 es un diagrama de bloques que ilustra una realización ilustrativa de la presente invención.
Las figuras 2a y 2b son un diagrama de flujo ilustrativo por el que un dispositivo de límite autorizado recibe el contenido en la realización de la figura 1.
Las figuras 3a y 3b son un diagrama de flujo ilustrativo por el que un dispositivo autorizado transfiere el contenido a otro dispositivo autorizado en la realización de la figura 1.
Las figuras 4a y 4b son un diagrama de flujo ilustrativo por el que un dispositivo autorizado usa el contenido en la realización de la figura 1.
La figura 5 es un diagrama de bloques de una realización ilustrativa de la presente invención que emplea un proveedor de gestión de confianza.

Descripción detallada de la invención

El sistema de protección de contenidos de la presente invención proporciona un medio flexible para permitir que los proveedores de contenidos establezcan los usos permitidos de un contenido con licencia. Está construido alrededor de un marco lógico de dispositivos autorizados y dominios autorizados. Los dispositivos autorizados son simplemente dispositivos que contienen el software y/o el hardware necesarios para cumplir con el sistema desvelado. Los dominios autorizados son grupos de dispositivos autorizados propiedad de un usuario. La inclusión de dominios autorizados en el sistema de protección de contenidos de la presente invención proporciona

distribuidores de contenido con un límite razonable para limitar la libertad de los usuarios para usar sus contenidos.

La figura 1 es un diagrama de bloques que ilustra una realización ilustrativa de la presente invención. De acuerdo con la presente invención, los proveedores de contenidos 50 distribuyen contenidos a los clientes que reciben los contenidos en los dispositivos autorizados compatibles, como el dispositivo autorizado A 12, o en los dispositivos heredados no compatibles, como el dispositivo heredado 20. Los proveedores de contenidos pueden distribuir sus contenidos en cualquier número de formas, tales como la transmisión vía satélite 51, internet 52 (vía reproducción directa o descarga), medios pre-grabados 53 (como los CD-ROM), una emisión tradicional 54, o similares.

Cualquier dispositivo usado para reproducir o grabar contenidos puede ser un dispositivo autorizado. El único factor que distingue los dispositivos autorizados de otros dispositivos es que los dispositivos autorizados están diseñados o programados para cumplir con el sistema de protección de contenidos de la presente invención. Los dispositivos contienen, en general, una CPU, una RAM, una memoria a largo plazo, y un método para comunicarse con otros dispositivos. Los ejemplos de posibles dispositivos autorizados incluyen videograbadoras digitales (DVR), receptores de TV, reproductores/grabadoras de DVD, ordenadores personales, asistentes digitales personales, receptores estéreo, reproductores/grabadoras de CD, reproductores/grabadoras de minidisco, reproductores/grabadoras de DAT, videocámaras digitales, etc.

Un destinatario de contenidos que participa en el sistema de protección de contenidos tendría uno o más dispositivos autorizados organizados en un dominio autorizado. El dominio autorizado representa alguna agrupación lógica de dispositivos. El dominio autorizado podría incluir la totalidad de los dispositivos de un individuo, los dispositivos de un hogar o los dispositivos de una empresa. El dominio autorizado podría ser cualquier agrupación de dispositivos que fuera adecuada para el usuario, o podría establecerse por la parte que gestiona el sistema de protección de contenidos. Cuando el gestor del sistema de protección de contenidos establece qué agrupación de dispositivos puede colocarse en un dominio autorizado, puede hacerlo limitando el número total de dispositivos incluidos en un dominio. O bien, puede establecer la relación entre los propietarios de los dispositivos en un dominio, por ejemplo, todos ellos deben vivir en la misma dirección.

Todavía en referencia a la figura 1, el dominio autorizado 10 muestra una posible disposición de un dominio autorizado. El dominio autorizado 10 comprende cinco dispositivos autorizados, el dispositivo autorizado A 12, el dispositivo autorizado B 13, el dispositivo autorizado C 14, el dispositivo autorizado D 15 y el dispositivo autorizado E 16. Todos estos dispositivos están conectados entre sí a través de la red local 11. En una realización ventajosa, la red local 11 sería una LAN que conecta los diversos dispositivos autorizados usando cualquier protocolo de redes e interfaz de hardware conocido, por ejemplo, TCP/IP, en una red ethernet cableada o inalámbrica. Sin embargo, no es necesaria una red local en toda regla. El requisito básico solo es que un dispositivo autorizado en el dominio autorizado tenga una forma de transferir archivos entre el mismo y otro dispositivo autorizado. Este mecanismo para transferir archivos podría ser cualquiera, desde una conexión de bus serie universal (USB) a un simple disquete.

El dispositivo autorizado A 12 y el dispositivo autorizado E 16 son dispositivos de límite debido a que pueden recibir contenidos desde el exterior del dominio autorizado 10. Y, si el indicador de desplazamiento de dominio lo permite, pueden transferir archivos fuera del dominio.

Por ejemplo, el dispositivo autorizado A 12 podría ser una DVR que puede recibir contenidos de televisión DVB por satélite 51. La DVR también podría tener conectividad a internet, lo que le da la posibilidad de enviar los programas grabados a otros dispositivos a través de internet. En tal escenario, el usuario del dominio autorizado 10 podría usar el dispositivo autorizado A 12 para enviar un programa que le guste al receptor de televisión digital de su amigo en el dominio autorizado 40. Por supuesto, esto solo funcionará si el indicador del estado de uso y el indicador de desplazamiento de dominio establecidos por la emisora DVB permiten este uso.

El funcionamiento del sistema se demuestra, además, mostrando cómo una persona que está viajando podría usar el sistema. En este ejemplo, el dispositivo autorizado E 16 es un reproductor de MP3 portátil y el dispositivo autorizado D 15 es un equipo de música doméstico con un disco duro para almacenar los archivos MP3 del usuario. Un usuario del dominio autorizado 10 podría, si lo permite el proveedor de contenidos, copiar los archivos MP3 del equipo de música al reproductor de MP3 portátil usando un sistema inalámbrico de corto alcance como el bluetooth. A continuación, podría disfrutar de la música en el reproductor portátil durante el vuelo a su destino. Tras la llegada, si se permiten los movimientos fuera del dominio autorizado, podría mover la música almacenada en el reproductor al equipo de música de su coche de alquiler en el dominio autorizado 30 para disfrutar mientras conduce.

COMPATIBILIDAD CON VERSIONES ANTERIORES

La compatibilidad con versiones anteriores es un aspecto importante en la ganancia de aceptación para cualquier nuevo esquema de protección de contenidos. La compatibilidad con versiones anteriores es importante debido al gran número de dispositivos no compatibles que se usan actualmente y la cantidad de tiempo necesario para conseguir un número significativo de dispositivos compatibles de uso público. En consecuencia, pocos proveedores de contenidos querrán adoptar un nuevo sistema si esto significa que tendrán que limitar su público a los pocos dispositivos compatibles que se han vendido.

El sistema actual podría implementarse de un manera que no fuera compatible con versiones anteriores. Por ejemplo, los proveedores de contenidos podrían distribuir sus contenidos de forma encriptada. Los dispositivos de límite autorizados tendrían las claves necesarias para desencriptar el contenido recibido. En función del método de distribución usado, estas claves podrían generarse cada vez que se transfiere el contenido, lo que sería un método ventajoso para las descargas de internet; o podrían almacenarse en el dispositivo autorizado y actualizarse de vez en cuando de una manera segura, lo que sería el método más útil para una DVB. Esta opción podría ser incluso preferible para algunos proveedores de contenidos que están dispuestos a renunciar a la compatibilidad con versiones anteriores para tener un control más estricto de sus contenidos.

La invención también puede implementarse de una manera que proporciona compatibilidad con versiones anteriores a través del uso de marcas de agua. Esto permitiría que el proveedor de contenidos distribuyera una información que mantiene las limitaciones de uso prescritas en los sistemas compatibles y que puede usarse en los sistemas heredados no compatibles.

El marcado con agua es un sistema en el que la información puede integrarse en el contenido sin ocultar el contenido. La marca de agua aplicada a una pieza del contenido puede ser perceptible o imperceptible según desee el proveedor de contenidos. El marcado con agua puede lograr esto sin dejar de ser robusto, es decir, la marca de agua no puede eliminarse del contenido, ya que es parte del contenido.

La naturaleza robusta del marcado con agua lo hace ideal para crear un sistema de protección de contenidos compatible con versiones anteriores. Las marcas de agua pueden usarse para identificar positivamente el contenido que está protegido por el sistema de protección de contenidos de la presente invención, distinguiéndolo, por lo tanto, del contenido heredado o no protegido. Sin una forma robusta de identificación del contenido protegido, los piratas podrían extraer la información de protección del contenido y confundir de este modo a los dispositivos autorizados para que traten al contenido protegido como un contenido heredado o no protegido. En un sistema que no usa el marcado con agua, esto podría lograrse simplemente eliminando la información de estado de uso y el indicador de desplazamiento de dominio del contenido. Con una marca de agua para identificar el contenido protegido, un dispositivo autorizado todavía reconocería el contenido como protegido incluso si se hubiera eliminado la información que identifica el nivel de protección. En tal caso, el dispositivo autorizado puede entonces asumir el contenido que se ha manipulado y aplicar la protección más estricta disponible.

Como se ha indicado anteriormente, el contenido marcado con agua no está completamente oscurecido y sigue siendo utilizable en los dispositivos heredados. Un ejemplo de una forma en crudo de marcado con agua visual sería colocar una gran marca opaca directamente sobre el contenido. Presumiblemente, los dispositivos autorizados serían capaces de eliminar esta marca, mediante el uso de la clave de marca de agua, cuando reproducen el contenido. Dicha marca limitaría notablemente el valor del contenido para los dispositivos heredados. El proveedor de contenidos puede elegir el nivel de obstrucción que desea usando marcas más pequeñas y/o translúcidas. Al decidir un nivel adecuado de obstrucción, el proveedor de contenidos puede equilibrar su deseo de proteger su contenido con su necesidad de servir a dispositivos heredados. Este equilibrio puede tener en cuenta su deseo de impulsar a los clientes a actualizar los dispositivos compatibles, o la naturaleza de los contenidos que se distribuyen.

En las situaciones en las que se requiere una paridad en la calidad de contenido entre los dispositivos compatibles y heredados, puede usarse la esteganografía para ocultar completamente la marca de agua. Esta técnica podría usarse por una cadena de televisión en la que hay una gran audiencia con dispositivos heredados que es poco probable que se actualicen para los equipos más actuales.

En una realización ventajosa de la presente invención, la marca de agua contendrá un ID de contenido que únicamente identifica el contenido. Este ID de contenido puede usarse entonces con la información de uso asociada al contenido. De esta manera, las restricciones de uso se vinculan firmemente al contenido al que se aplican. El ID de contenido impide que los usuarios eviten el esquema de protección sustituyendo la diferente información de uso que se usa con el contenido. Dicho intento fallará debido a que la información de uso sustituida no tendrá el ID de contenido correcto asociado a la misma. El ID de contenido puede vincularse firmemente a la restricción de uso a través del uso de las funciones de cálculo de clave, firmas digitales y/o cualquier otra técnica conocida.

La agregación de un ID de contenido en la marca de agua y la asociación de ese mismo ID de contenido con la información de uso tiene la ventaja adicional de garantizar que la información de uso emitida por los proveedores de contenidos sigue siendo diversa. Sin este identificador único para la información de uso, las funciones de cálculo de clave aplicadas a la información de uso asociada a un contenido diferente volverían a valores similares. Una parte que trata de burlar el sistema podría a continuación aprender los valores de cálculo de clave adecuados para diferentes derechos de uso y vencer esta protección.

FUNCIONAMIENTO DEL SISTEMA

El funcionamiento básico del sistema de la presente invención se basa en técnicas criptográficas para proteger el contenido en un dispositivo autorizado. La protección comienza encriptando el contenido y creando un certificado asociado al contenido. El certificado contiene la clave para desencriptar el contenido, la información de estado de

uso y el indicador de desplazamiento de dominio. El estado de uso y el indicador de desplazamiento de dominio establecen cómo puede usarse el contenido. Los estados de uso pueden ir desde no restringido, que significa que se permite cualquier copia, movimiento o uso, a completamente restringido, lo que impediría copiar, mover o usar el contenido. La clave de encriptación de contenido almacenada en el certificado está protegida de manera que los piratas no puedan apropiarse indebidamente de la misma y usarla para crear versiones sin licencia de los contenidos. La protección de clave de contenido se logra encriptando la propia clave o la totalidad del certificado. En una realización ventajosa, solo se encripta la clave de contenido. Los otros elementos del certificado se protegen de la manipulación, pero siguen siendo legibles. Esto puede lograrse, por ejemplo, usando una función de cálculo de clave criptográfica y, a continuación, firmando el cálculo de clave encriptándolo con la clave privada del dispositivo. Mantener partes del certificado legibles cuando el contenido es inaccesible tiene la ventaja de ofrecer a los usuarios información sobre por qué ha fallado su intento de uso. En un modelo de superdistribución la información legible podría decir al usuario cómo obtener un derecho de uso del contenido. Puede añadirse una encriptación adicional para garantizar niveles más altos de seguridad.

Las figuras 2a y 2b muestran un método ilustrativo por el que un dispositivo de límite autorizado recibe un contenido en la realización de la figura 1. En el bloque 200, el dispositivo recibe un contenido. En el bloque 210, el dispositivo comprueba una marca de agua que identificaría el contenido como protegido.

Si no hay marca de agua, el dispositivo trata el contenido como un contenido no protegido o heredado en el bloque 212. Esto podría incluir la creación de un certificado que establece que el estado de uso y el desplazamiento de dominio no están restringidos en absoluto, pero la creación de un certificado no es estrictamente necesaria. Usar un certificado para el contenido no protegido permitiría a los diseñadores eliminar los procedimientos de detección por marca de agua de los dispositivos no límites. En lugar de comprobar las marcas de agua, los dispositivos no límites podrían simplemente rechazar cualquier contenido no certificado.

Si el contenido está marcado con agua, se ejecuta el bloque 220 y se crea una clave de contenido y el contenido se encripta con la misma. Esta etapa de encriptación puede lograrse mediante cualquiera de las técnicas conocidas, tales como RC-5, IDEA, Blowfish, Cast-n, Misty, Skipjack, AES, 3-DES. Para garantizar un funcionamiento eficiente es muy probable que se logre usando un algoritmo criptográfico simétrico, como AES. Si la marca de agua es perceptible, esta etapa también podría incluir eliminar la parte perceptible de la marca de agua. Como alternativa, la marca de agua podría eliminarse cuando se reproduzca el contenido.

La creación de la clave de contenido puede lograrse generando aleatoriamente la clave o usando un valor inicial de clave de contenido transmitido con el contenido. Enviar un valor inicial de clave de contenido con el contenido permite que el proveedor de contenido conozca la clave de contenido que se usará para encriptar el contenido sin emitir la clave de contenido en sí. El proveedor de contenidos logra esto enviando un ID de contenido junto con el valor inicial de clave de contenido. El valor inicial de clave de contenido y el ID de contenido se asocian entre sí de una manera solo conocida por el proveedor de contenidos. Tras la recepción del valor inicial de clave de contenido, un dispositivo autorizado genera una clave de contenido encriptando el valor inicial de clave de contenido con su clave de dominio. Después de crear la clave de contenido, se descarta el valor inicial de clave de contenido y ya no se usa por el dispositivo receptor. Cuando el dispositivo crea un certificado asociado al contenido, se incluyen en el certificado el ID de contenido y un ID de dominio que identifica su dominio. Si el proveedor de contenidos nunca necesita la clave de contenido, puede usar el ID de contenido y el ID de dominio incluidos en el certificado para buscar el valor inicial de clave de contenido y la clave de dominio. A continuación, puede realizar la misma operación realizada por el dispositivo autorizado para restablecer la clave de contenido.

Ofrecer al proveedor de contenidos la posibilidad de recrear la clave de contenido es útil por al menos tres razones. Si se pierde o se destruye la clave de contenido asociada al contenido, el proveedor de contenidos puede restablecer la clave y crear un nuevo certificado para el contenido. Si el contenido se transfiere a un dispositivo en el que no puede usarse, el proveedor de contenidos podría emitir un certificado válido para el contenido. Esta es una manera de permitir la superdistribución. Distribuir el valor inicial de clave de contenido en lugar de la clave de contenido en sí tiene la ventaja de evitar la necesidad de proteger la clave de contenido en tránsito, y crea una manera fácil de garantizar que los diferentes dominios tengan claves de contenido diferentes.

El bloque 230 comprueba el indicador de desplazamiento de dominio para determinar si se permite el desplazamiento de dominio. Si no se permite el desplazamiento de dominio, lo que significa que la información no puede enviarse fuera del dominio autorizado, la clave de contenido se encripta con una clave de dominio en el bloque 235. La clave de dominio es una clave compartida por todos los dispositivos en un dominio autorizado. Tener la misma clave de dominio es lo que define a los dispositivos como parte de un único dominio.

El bloque 240 comprueba la información de estado de uso asociada al contenido. En la mayoría de los casos, la información de estado de uso se transmitirá con el contenido y tendrá un ID de contenido asociado, que coincidirá con un ID de contenido incluido en la marca de agua. La información de estado de uso puede tener varias configuraciones diferentes, siendo algunos posibles estados de uso:

No restringido
Copiar X veces
Copiar una vez
No copiar más
No copiar nunca
No copiar nunca, no mover nunca

Si el estado de uso es cualquier otro distinto del no restringido, la clave de contenido se encripta en el bloque 245 usando la clave pública del dispositivo receptor. Como es habitual en los sistemas criptográficos de clave pública, la encriptación con la clave pública de este dispositivo garantiza que solo la clave privada de este dispositivo puede desencriptar la clave de contenido. Puesto que el contenido se inutilizará a menos que este dispositivo desencripte la clave de contenido, esta etapa garantiza que el dispositivo controlará cualquiera de los contenidos. Si el uso no está restringido esta etapa es innecesaria.

Una alternativa para distribuir el estado de uso con el contenido es hacer que la información sea implícita. En este sistema, los usos permitidos del contenido se añaden por el dispositivo receptor en lugar de transmitirse con el contenido. Esto evita la necesidad de descargar la información de estado de uso con el contenido. Este sistema, sin embargo, carece de la flexibilidad del sistema descrito anteriormente porque todos los contenidos tendrían la misma información de estado de uso. Este sistema podría hacerse un sistema algo más flexible usando algunos estados de uso diferentes que se aplican basándose en otros criterios. Por ejemplo, en el contexto de la DVB podrían aplicarse diferentes estados de uso basándose en el canal del programa en que se ha emitido. En este escenario, las redes ordinarias podrían tener estados de uso libre, pero los canales de pago por visión podrían aplicar los estados de uso disponibles más estrictos.

El bloque 250 crea un certificado que contiene la clave de contenido encriptada, el estado de uso, el ID de contenido y el indicador de desplazamiento de dominio. Para mejorar la seguridad, el certificado puede protegerse para garantizar que un pirata no modifique la información de estado de uso. Esto podría lograrse a través del uso de una función de cálculo de clave criptográfica y una firma digital.

Por último, el bloque 260 almacena el certificado y el contenido encriptado en el dispositivo.

Una revisión cuidadosa del proceso recién descrito mostrará que la clave de contenido se encripta basándose en el tipo de protección declarada. Si, por ejemplo, la copia no está restringida, pero no se permite la transmisión fuera del dominio, solo podrá usarse la clave de dominio para encriptar la clave de contenido. Encriptar la clave de contenido basándose en la protección declarada simplifica el redireccionamiento del contenido a otros dispositivos. Por ejemplo, redirigir un contenido cuyo uso está restringido y cuyo desplazamiento de dominio está prohibido implicaría, simplemente, una comprobación para ver si el dispositivo de destino está dentro del dominio y, a continuación, enviar el contenido y el certificado al dispositivo de destino. No se necesitan otras operaciones. Incluso podría omitirse la etapa de comprobar si el dispositivo de destino está en el dominio, debido a que un dispositivo fuera del dominio no tendría el requisito de clave de dominio, por lo que el contenido encriptado sería inutilizable.

La situación recién descrita es especialmente ventajosa, debido a que el uso restringido y el desplazamiento de dominio prohibido es probable que sea la primera configuración elegida por los proveedores de contenidos. De hecho, podría ser la única configuración que los proveedores de contenidos necesitaran implementar. Este nivel de protección logra un equilibrio entre la protección de contenidos contra la piratería generalizada y el mantenimiento de un nivel muy poco restringido de uso para los clientes con licencia.

Las figuras 3a y 3b son un diagrama de flujo ilustrativo por el que un dispositivo autorizado mueve o copia un contenido recibido previamente a otro dispositivo autorizado en la realización de la figura 1. En el bloque 300, se inicia la transferencia.

En el bloque 310, el dispositivo de transferencia comprueba si el dispositivo de destino está dentro del dominio. Si no lo está, el indicador de desplazamiento de dominio en el certificado se comprueba en el bloque 312 para ver si se permite el desplazamiento de dominio. Si no se permite, la solicitud se rechaza en el bloque 318. Como era de imaginar, los bloques 310, 312 y 318 no son estrictamente necesarios porque, incluso si un dispositivo fuera del dominio recibe el contenido, no será capaz de usarlo sin la clave de desplazamiento de dominio. La única ventaja de estas etapas es que evitan rápidamente el resto del procedimiento si se prohíbe el desplazamiento de dominio.

En el bloque 320, se comprueba el estado de uso de certificado. Si el uso está restringido, el proceso avanza inmediatamente al bloque 360 para transferir el certificado y el contenido. Si el estado de uso indica que el uso está restringido de alguna manera, se comprueba el estado de uso en el bloque 330 para ver si se permite la operación solicitada. Si no se permite, se rechaza la solicitud en el bloque 335. Si se permite la operación solicitada, debe redirigirse la clave de contenido. En el bloque 340, la clave de contenido se desencripta usando la clave privada del dispositivo de transferencia. A continuación, en el bloque 350, la clave de contenido se encripta usando la clave pública del dispositivo de destino. Esta clave de contenido recién encriptada se usa como parte de un certificado redirigido para enviarse al nuevo dispositivo.

En el bloque 355, se realizan todos los cambios necesarios en la información de estado de uso. Por ejemplo, si el estado de uso era copiar X veces, donde X es un número entero positivo, X se reduce en 1. Si X era 1, el estado de uso se convierte en no copiar más. No copiar más y no copiar nunca son esencialmente lo mismo, excepto que no copiar más podría usarse para indicar que se contacta con el proveedor de contenidos para adquirir privilegios de uso adicionales. El estado de copiar una vez mencionado anteriormente es idéntico a copiar X, donde X es igual a 1.

El bloque 355 también es el primer lugar en el que la diferencia entre copiar y mover se vuelve relevante. Copiar indica la creación de un duplicado del archivo en el que la transferencia y el dispositivo de destino conservan una copia del archivo. Por el contrario, mover indica que el dispositivo de transferencia no conserva una copia del archivo. Permitir siempre el movimiento sería una manera de hacer que el contenido digital protegido cumpliera con la primera doctrina de ventas de la ley de derechos de autor.

Con respecto a la etapa 355, si se ha solicitado un movimiento, no se haría nada a menos que, por supuesto, se haya implementado otro control de uso que restrinja el número de movimientos (la implementación de este control sería similar a copiar X). Si se solicita una copia, el certificado retenido en el dispositivo de transferencia debe actualizarse como se ha descrito anteriormente, y debe crearse una nueva información de estado de uso para el certificado redirigido. El certificado redirigido probablemente ofrecería un estado de uso de no copiar más para evitar la proliferación de copias, pero también podría conseguir una copia del estado de uso recién actualizado del original. El certificado redirigido tiene, normalmente, el mismo indicador de desplazamiento de dominio que el certificado original.

A continuación, en el bloque 360, el contenido y el certificado se envían al dispositivo de destino. Este es o el certificado redirigido o una copia del certificado original si se ha seguido la rama del sí del bloque 320.

Por último, si se determina en el bloque 365 que la transferencia solicitada era un movimiento, a continuación, en el bloque 370 se borran el contenido y el certificado, o se hacen inaccesibles o ilegibles de otro modo, en el dispositivo de transferencia. El bloque 375 marca el final de la rutina.

Las figuras 4a y 4b son un diagrama de flujo ilustrativo por el que un dispositivo autorizado usa contenidos en la realización de la figura 1. El proceso comienza en el bloque 400 con una solicitud de reproducción. En el bloque 410, se comprueba el registro de estados de uso en el certificado. En los bloques 420 y 425, se hacen cumplir los límites de reproducción. Esto puede requerir simplemente que unos estados de uso adicionales establezcan si el contenido puede reproducirse o no, o cuántas veces puede reproducirse el contenido. Obviamente, los bloques 420 y 425 se eliminan si no hay restricciones de reproducción. En el bloque 430, se desencripta la clave de contenido en el certificado con la clave privada del dispositivo. Este bloque, sin embargo, solo se alcanza si el estado de uso no está restringido. De lo contrario, no se habría encriptado la clave de contenido con la clave pública del dispositivo.

En el bloque 440, se comprueba el indicador de desplazamiento de dominio. Si se prohíbe el desplazamiento de dominio, la clave de contenido debe desencriptarse en el bloque 450 con la clave de dominio. La clave de contenido ya está legible y el contenido puede desencriptarse en el bloque 460. Obsérvese que si el contenido estuviera completamente desprotegido no se encriptaría, por lo que no sería necesario desencriptar el contenido. Por último, en el bloque 470, el dispositivo reproduce el contenido.

La figura 5 es un diagrama de bloques que representa una realización ilustrativa de la presente invención, similar a la realización de la figura 1, pero que también incluye un proveedor de gestión de confianza 500. El proveedor de gestión de confianza facilita algunas de las transacciones más complejas que se permiten por la presente invención.

La presente invención podría usarse como un esquema de protección de contenidos integral para cualquier tipo de contenido o de dispositivo. En esta realización ventajosa, implementarían el sistema una multitud de proveedores de contenidos y fabricantes de dispositivos. Sin embargo, con un sistema tan generalizado, podría ser que no todas las diversas implementaciones diferentes del esquema de protección de contenidos funcionaran de la misma manera. En este escenario, puede interponerse un tercero de confianza en forma de un proveedor de gestión de confianza para garantizar que las diversas implementaciones permanecen interoperables.

En la práctica, el proveedor de gestión de confianza 500 puede implementarse a través del uso de un servidor que puede comunicarse con los dispositivos necesarios y que está programado para hacer cumplir las reglas del sistema.

Haciendo referencia a la figura 5, todos los diversos dispositivos autorizados 12-16 en el dominio autorizado 10 podrían fabricarse por diferentes entidades. En consecuencia, cuando un usuario del dominio agrega un nuevo dispositivo al dominio, puede consultarse al proveedor de gestión de confianza 500 para certificar que el nuevo dispositivo cumple las normas requeridas por el sistema. Este proceso podría incluir la comunicación con un tercero que establece las normas para crear dominios para este usuario; por ejemplo un proveedor de contenidos. Como alternativa, el proveedor de gestión de confianza podría controlar todo el proceso de unión de dispositivos en los dominios autorizados y mantener los dominios creados. En esta función, el proveedor de gestión de confianza también podría reemplazar las claves de contenido inservibles producidas con valores iniciales de clave de

contenido, como se ha descrito anteriormente. El proveedor de gestión de confianza también podría proporcionar información a los otros dispositivos en el dominio relativo al funcionamiento del nuevo dispositivo.

El proveedor de gestión de confianza también puede usarse para facilitar las transferencias inter-dominio, por ejemplo, entre los dominios autorizados 10 y 40. Ambos dominios autorizados 10 y 40 podrían contener los dispositivos que reciben y almacenan los contenidos DVB. Sin embargo, si reciben su contenido de diferentes proveedores, por ejemplo, diferentes compañías de cable, podrían surgir problemas con la transferencia. Los proveedores de contenidos podrían querer garantías de que el contenido se protegería adecuadamente en el otro dominio. El proveedor de gestión de confianza podría comprobar los requisitos del proveedor de contenidos y, a continuación, determinar si el dominio receptor los cumple. O bien, el proveedor de contenidos puede exigir el pago si el contenido se transfiere al usuario de un servicio diferente. El proveedor de gestión de confianza también puede coordinar el pago, como se verá a continuación.

El uso de un proveedor de gestión de confianza puede facilitar las transacciones comerciales y la legibilidad de uso que implican los contenidos protegidos. Por ejemplo, en un modelo de superdistribución, cuando el contenido se envía desde el dominio de un usuario al de otro, pueden generarse muchos pagos. Un ejemplo concreto ilustrará algunos pagos posibles y la utilidad del proveedor de gestión de confianza. El usuario A descarga algo de música desde un proveedor de contenidos a través de Internet y paga por el uso del contenido. A continuación, transfiere una copia del contenido a un amigo, el usuario B, en un dominio autorizado diferente. El usuario B recibe el contenido, lo escucha para probar y decide comprar los derechos de uso para sí mismo. El proveedor de gestión de confianza puede garantizar que las partes siguientes reciben parte del pago: El usuario A podría obtener una parte por enviar el contenido al usuario B, el proveedor de contenidos obtendrá una parte, y el creador de contenidos obtendrá una parte. El uso de un proveedor de gestión de confianza como una tercera parte neutral de confianza garantiza que todas las transacciones se justifican adecuadamente.

Las numerosas características y ventajas de la presente invención son evidentes a partir de la memoria descriptiva detallada y, por lo tanto, mediante las reivindicaciones adjuntas se pretenden cubrir todas estas características y ventajas de la invención que están comprendidas en el ámbito de la invención.

Además, puesto que a los expertos en la materia se les ocurrirán fácilmente numerosas modificaciones y variaciones, no se desea que la presente invención esté limitada a la instrucción y el funcionamiento exactos ilustrados y descritos en el presente documento. En consecuencia, se pretende que todas las modificaciones adecuadas a las que puede recurrirse estén comprendidas en el ámbito de las reivindicaciones.

REIVINDICACIONES

1. Un método para mover contenidos protegidos dentro de un dominio autorizado (10), en el que al menos un primer dispositivo (12) y un segundo dispositivo (13) forman parte del dominio autorizado, compartiendo cada uno de los dispositivos (12, 13) que forman parte del dominio autorizado una clave de dominio, en el que tener la clave de dominio define los dispositivos (12, 13) como parte del dominio autorizado, comprendiendo el método con respecto al primer dispositivo:

recibir de una fuente de proveedor de contenidos externa (50) un valor inicial de clave de contenido y un contenido que comprende un ID de contenido, en donde el valor inicial de clave de contenido y el ID de contenido están asociados entre sí de una manera conocida por el proveedor de contenidos;
crear una clave de contenido operando sobre el valor inicial de clave de contenido con la clave de dominio del primer dispositivo;
encriptar el contenido recibido con la clave de contenido;
encriptar la clave de contenido con la clave de dominio, de tal manera que todos los dispositivos dentro del dominio autorizado tengan la capacidad de desencriptar la clave de contenido encriptada con la clave de dominio;
crear un certificado asociado al contenido encriptado, incluyendo el certificado la clave de contenido encriptada, el ID de contenido, un registro de estados de uso que establece los límites de reproducción en relación con el contenido, y la información que identifica el dominio autorizado;
transmitir el contenido encriptado y el certificado al segundo dispositivo (13); y
después de transmitir el certificado, inutilizar cualquier certificado en el primer dispositivo que esté asociado a dicho contenido encriptado.

2. El método de la reivindicación 1 que comprende además:

encriptar la totalidad del certificado en el primer dispositivo.

3. El método de las reivindicaciones 1 o 2 que comprende además:

recibir en el segundo dispositivo dicho contenido encriptado y el certificado asociado a ese contenido.

4. El método de las reivindicaciones 1, 2 o 3 que comprende con respecto al segundo dispositivo:

desencriptar la clave de contenido encriptada; y
usar la clave de contenido desencriptada para desencriptar el contenido encriptado.

5. Un programa informático que comprende unas instrucciones de programa informático que, cuando son ejecutadas por un aparato, hacen que dicho aparato realice un método de acuerdo con la reivindicación 1 o la reivindicación 2.

6. Un aparato (12) para mover contenidos protegidos dentro de un dominio autorizado (10), en el que al menos un primer dispositivo (12) y un segundo dispositivo (13) forman parte del dominio autorizado, compartiendo cada uno de los dispositivos (12, 13) que forman parte del dominio autorizado una clave de dominio, en el que tener la clave de dominio define los dispositivos (12, 13) como parte del dominio autorizado, comprendiendo el aparato:

medios para recibir en el primer dispositivo desde una fuente de proveedor de contenidos externa (50) un valor inicial de clave de contenido y un contenido que comprende un ID de contenido, que están asociados entre sí de una manera conocida por el proveedor de contenidos;
medios para crear, en el primer dispositivo, una clave de contenido operando sobre el valor inicial de clave de contenido con la clave de dominio del primer dispositivo;
medios para encriptar, en el primer dispositivo, el contenido recibido con una clave de contenido;
medios para encriptar, en el primer dispositivo, la clave de contenido con la clave de dominio, de tal manera que todos los dispositivos dentro del dominio autorizado tengan la capacidad de desencriptar la clave de contenido encriptada con la clave de dominio;
medios para crear, en el primer dispositivo, un certificado asociado al contenido encriptado, incluyendo el certificado la clave de contenido encriptada, el ID de contenido, un registro de estados de uso que establece los límites de reproducción en relación con el contenido, y la información que identifica el dominio autorizado;
medios para transmitir el contenido encriptado y el certificado desde el primer dispositivo al segundo dispositivo (13); y
medios para inutilizar cualquier certificado en el primer dispositivo que esté asociado a dicho contenido encriptado, después de transmitir el certificado.

7. El aparato de la reivindicación 6, que comprende además:

medios para encriptar, en el primer dispositivo, la totalidad del certificado.

Figura 1

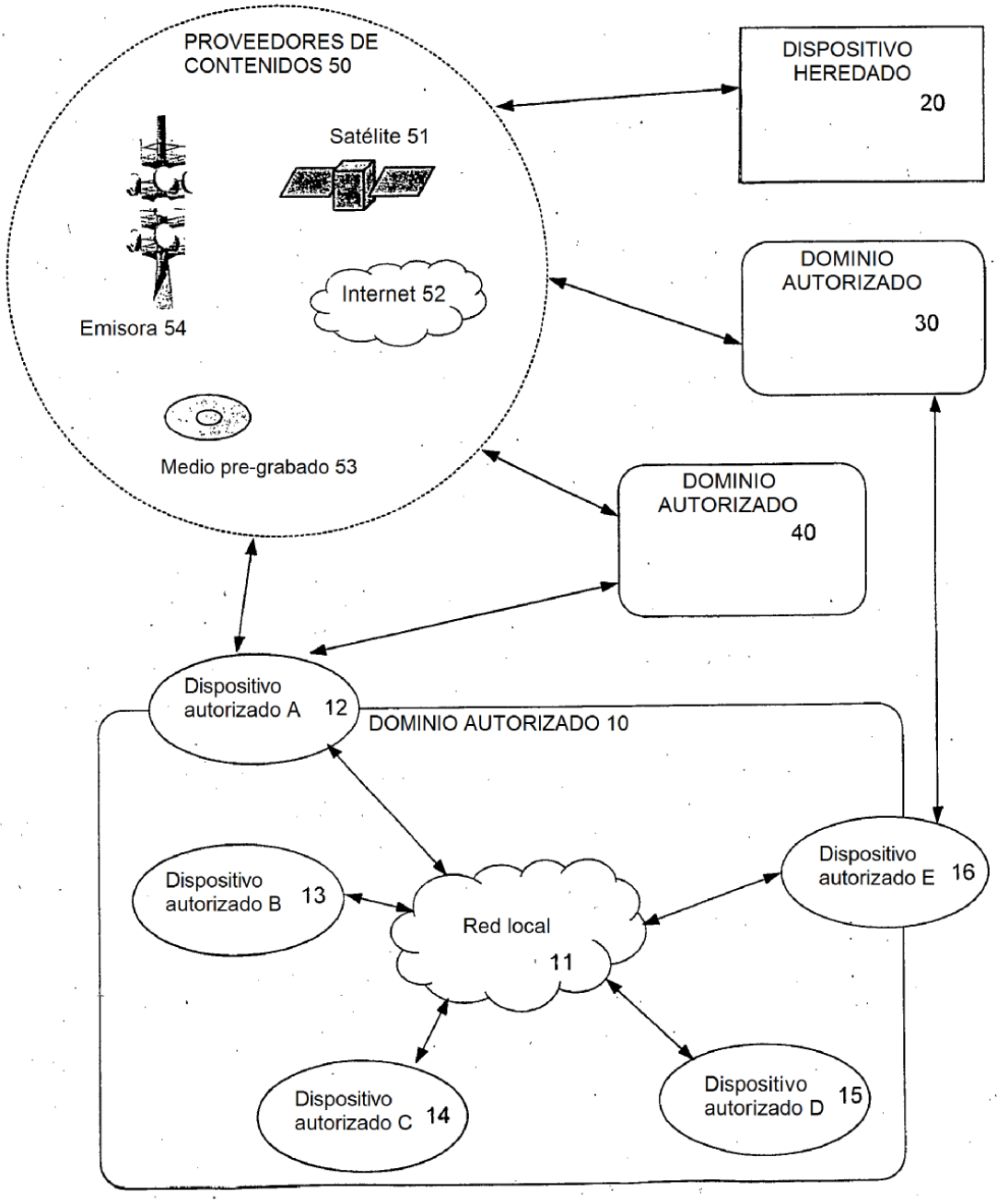

PROVEEDORES DE CONTENIDOS 50
Satélite 51
Internet 52
Emisora 54
Medio pre-grabado 53
DISPOSITIVO HEREDADO 20
DOMINIO AUTORIZADO 30
DOMINIO AUTORIZADO 40
Dispositivo autorizado A 12
DOMINIO AUTORIZADO 10
Dispositivo autorizado B 13
Red local 11
Dispositivo autorizado E 16
Dispositivo autorizado C 14
Dispositivo autorizado D 15

Figura 2a

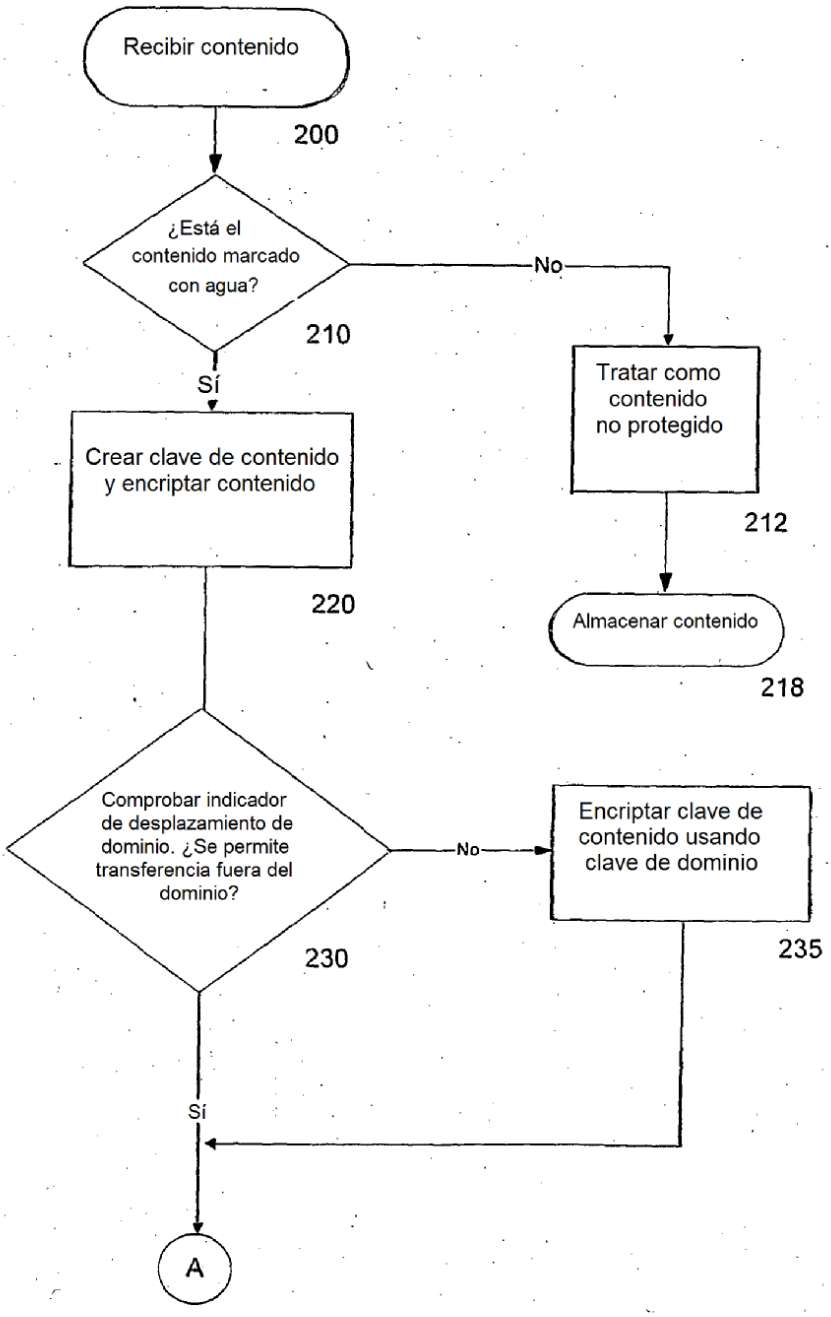

Recibir contenido
200
¿Está el contenido marcado con agua?
210
No
Sí
Tratar como contenido no protegido
212
Crear clave de contenido y encriptar contenido
220
Almacenar contenido
218
Comprobar indicador de desplazamiento de dominio. ¿Se permite transferencia fuera del dominio?
230
No
Encriptar clave de contenido usando clave de dominio
235
Sí
A

Figura 2b

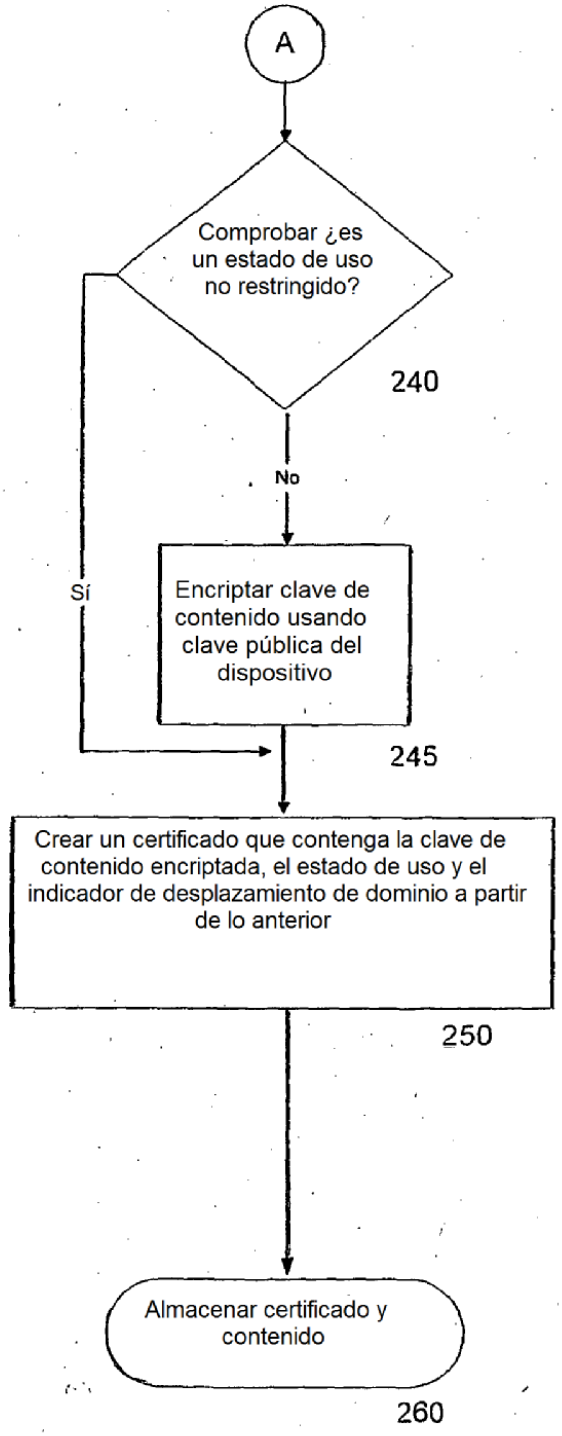

A
Comprobar ¿es un estado de uso no restringido?
240
No
Sí
Encriptar clave de contenido usando clave pública del dispositivo
245
Crear un certificado que contenga la clave de contenido encriptada, el estado de uso y el indicador de desplazamiento de dominio a partir de lo anterior
250
Almacenar certificado y contenido
260

Figura 3a

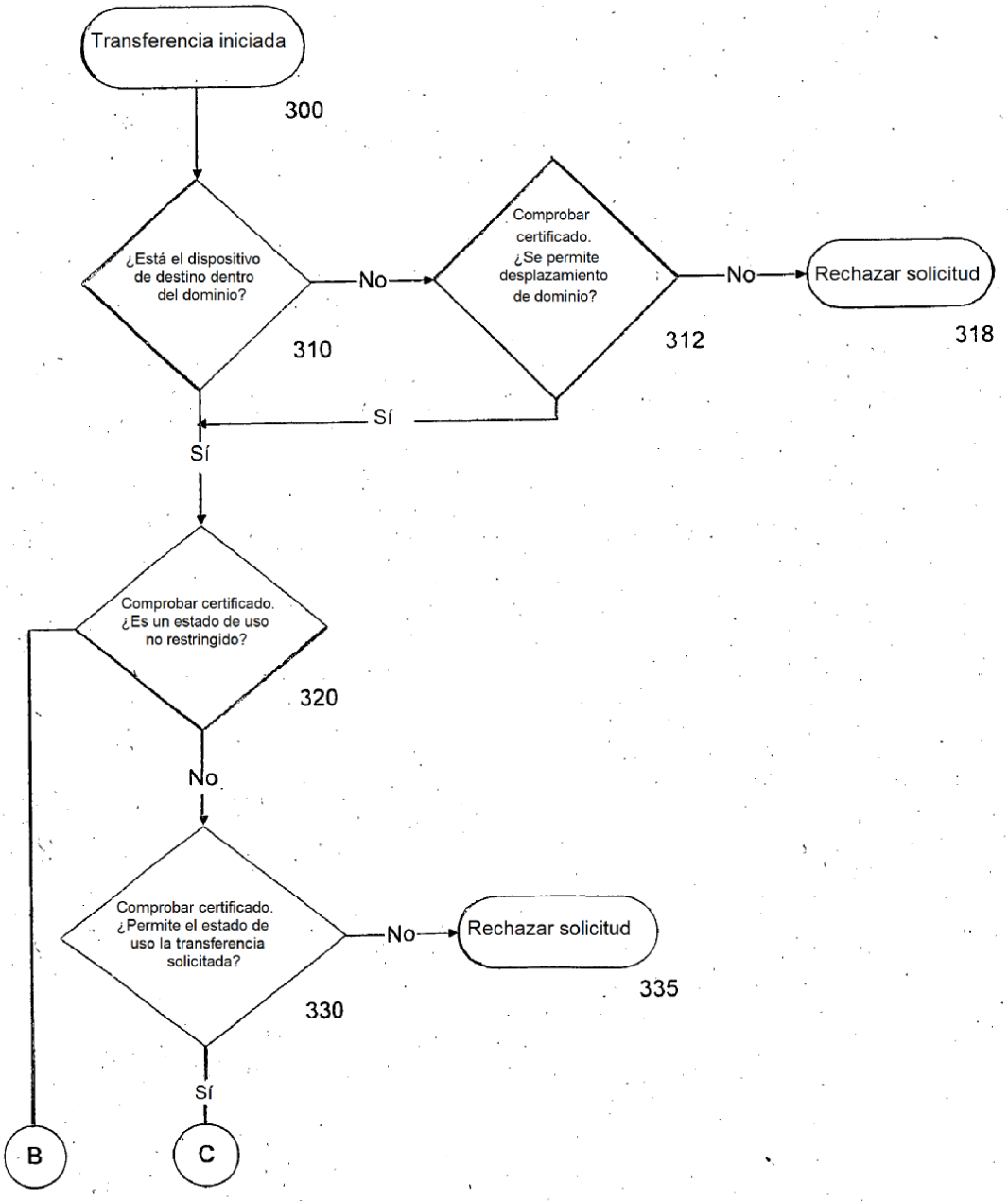

Transferencia iniciada
300
¿Está el dispositivo de destino dentro del dominio?
310
No
Comprobar certificado. ¿Se permite desplazamiento de dominio?
312
No
Rechazar solicitud
318
Sí
Sí
Comprobar certificado. ¿Es un estado de uso no restringido?
320
No
Comprobar certificado. ¿Permite el estado de uso la transferencia solicitada?
330
No
Rechazar solicitud
335
Sí
B
C

Figura 3b

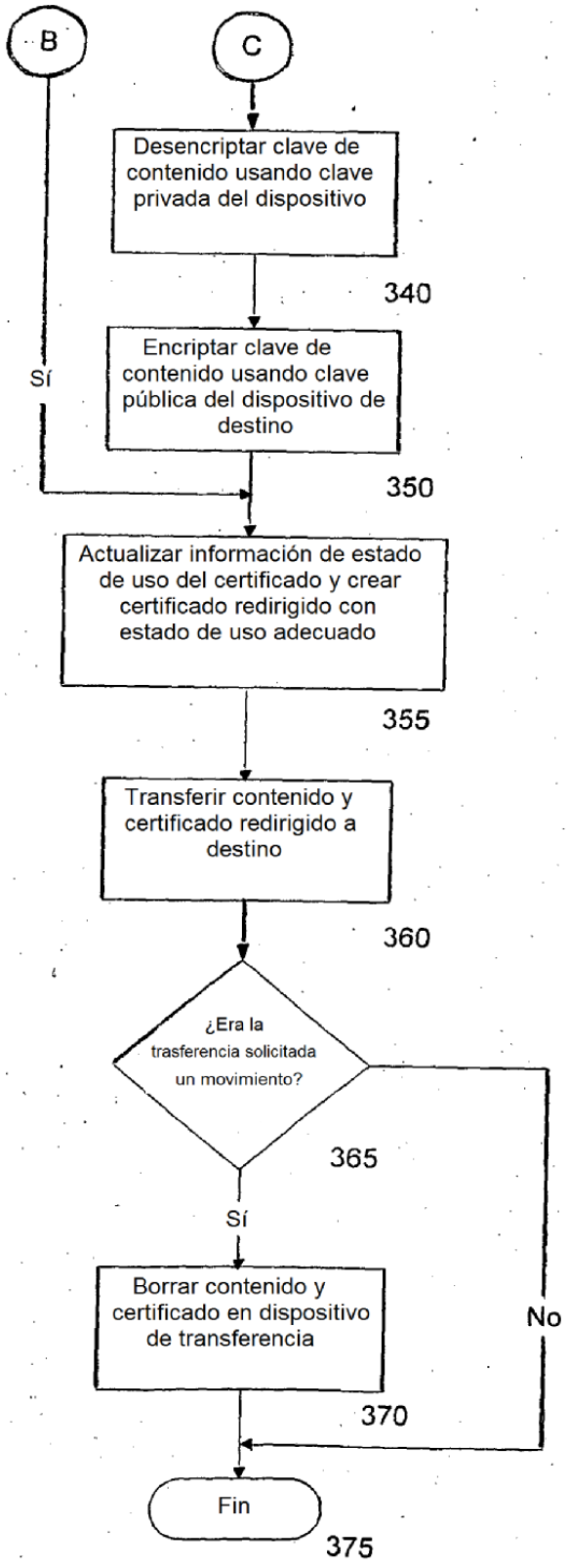

B
C
Desencriptar clave de contenido usando clave privada del dispositivo
340
Encriptar clave de contenido usando clave pública del dispositivo de destino
Sí
350
Actualizar información de estado de uso del certificado y crear certificado redirigido con estado de uso adecuado
355
Transferir contenido y certificado redirigido a destino
360
¿Era la trasferencia solicitada un movimiento?
365
Sí
No
Borrar contenido y certificado en dispositivo de transferencia
370
Fin
375

Figura 4a

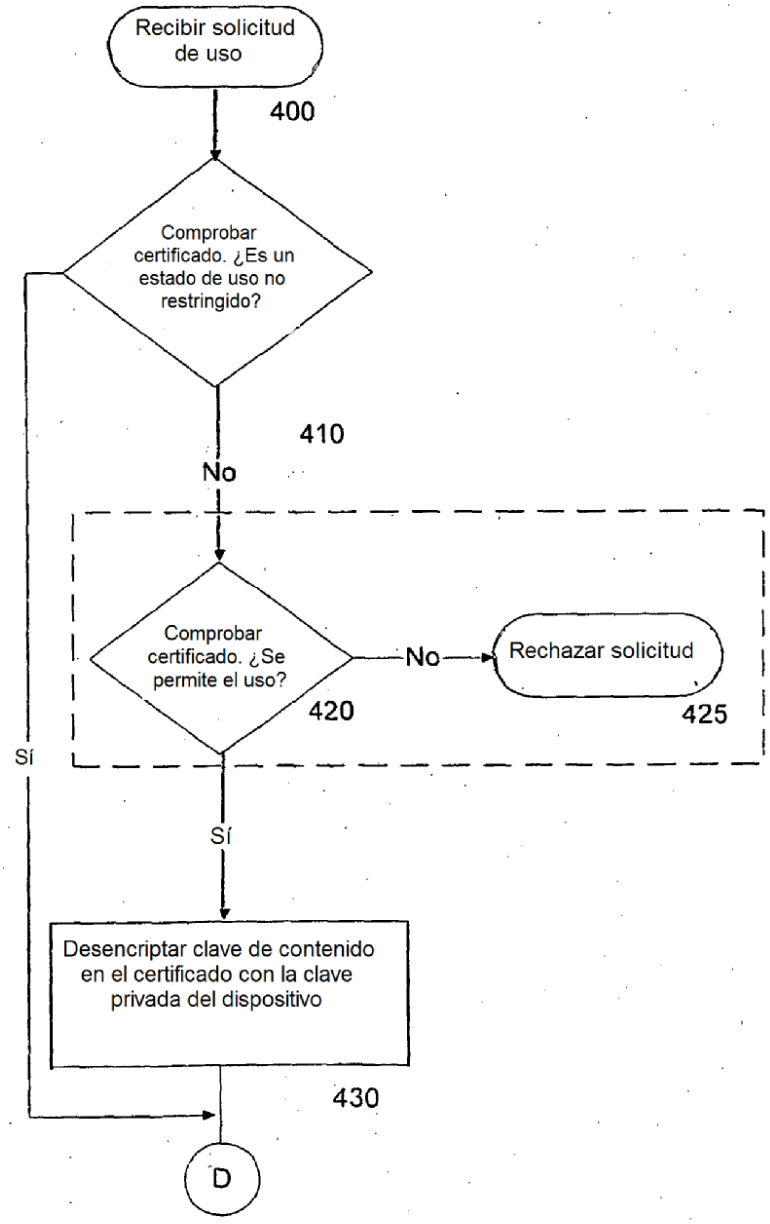

Recibir solicitud de uso
400
Comprobar certificado. ¿Es un estado de uso no restringido?
410
No
Comprobar certificado. ¿Se permite el uso?
420
No
Rechazar solicitud
425
Sí
Sí
Desencriptar clave de contenido en el certificado con la clave privada del dispositivo
430
D

Figura 4b

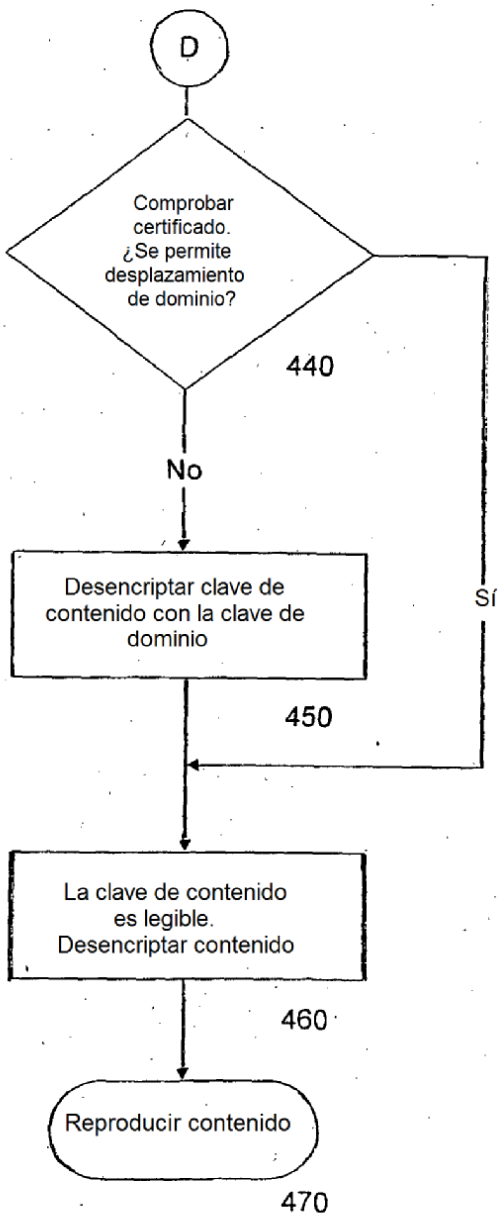
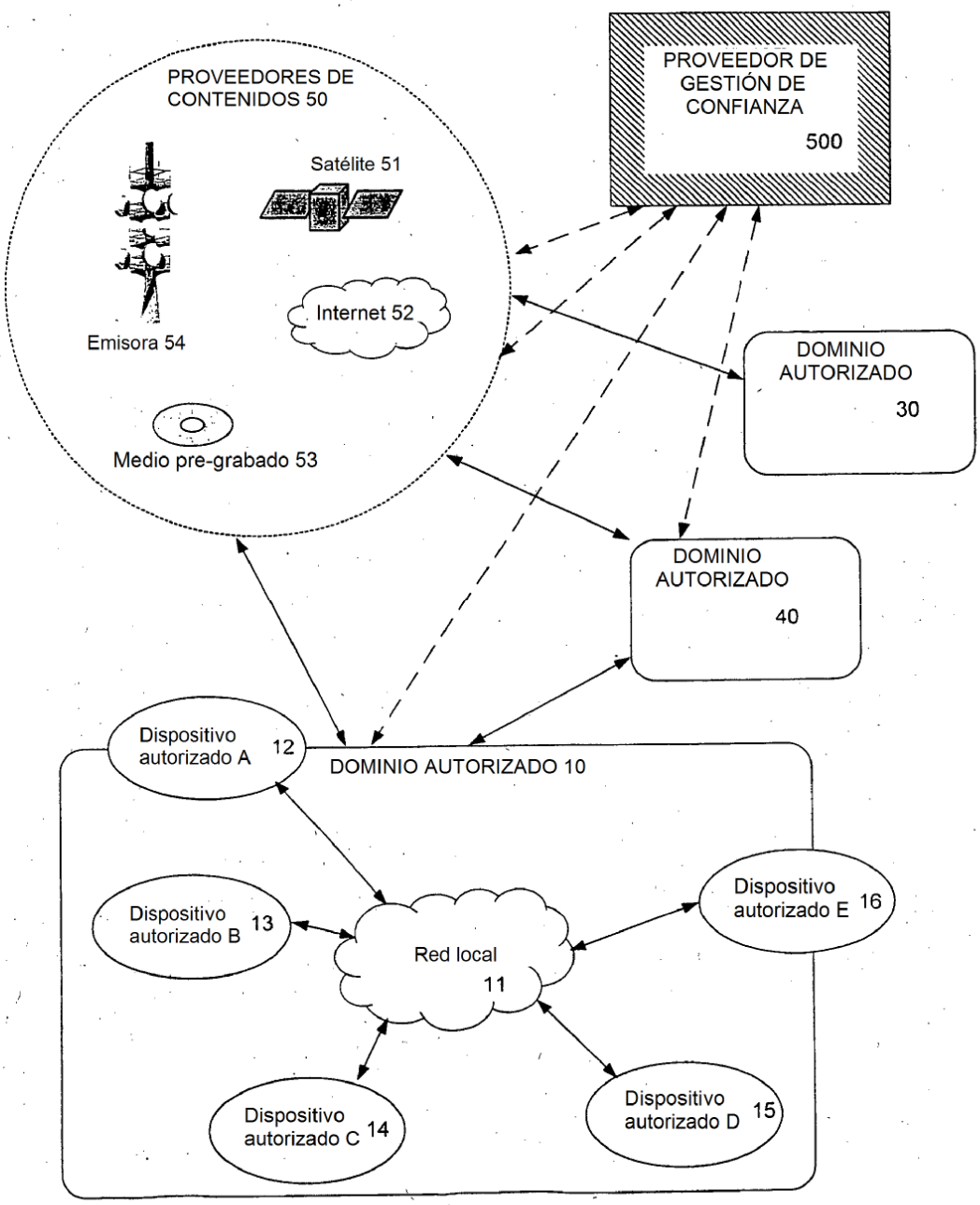

D
Comprobar certificado. ¿Se permite desplazamiento de dominio?
440
No
Sí
Desencriptar clave de contenido con la clave de dominio
450
La clave de contenido es legible. Desencriptar contenido
460
Reproducir contenido
470

Figura 5


PROVEEDORES DE CONTENIDOS 50
Satélite 51
Internet 52
Emisora 54
Medio pre-grabado 53
PROVEEDOR DE GESTIÓN DE CONFIANZA
500
DOMINIO AUTORIZADO
30
DOMINIO AUTORIZADO
40
Dispositivo autorizado A 12
DOMINIO AUTORIZADO 10
Dispositivo autorizado B 13
Red local
11
Dispositivo autorizado E 16
Dispositivo autorizado C 14
Dispositivo autorizado D 15