



19



OFICINA ESPAÑOLA DE
PATENTES Y MARCAS

ESPAÑA

11 Número de publicación: **2 273 314**

51 Int. Cl.:
H04L 12/28 (2006.01)

12

TRADUCCIÓN DE PATENTE EUROPEA

T3

86 Número de solicitud europea: **05251225 .8**

86 Fecha de presentación : **01.03.2005**

87 Número de publicación de la solicitud: **1571787**

87 Fecha de publicación de la solicitud: **07.09.2005**

54 Título: **Aparato y procedimiento para comunicar el estado de funcionamiento de la gestión de derechos digitales.**

30 Prioridad: **02.03.2004 US 548888 P**
02.04.2004 KR 10-2004-0022882

45 Fecha de publicación de la mención BOPI:
01.05.2007

45 Fecha de la publicación del folleto de la patente:
01.05.2007

73 Titular/es: **SAMSUNG ELECTRONICS Co., Ltd.**
416 Maetan-dong, Yeongtong-gu
Suwon-si, Gyeonggi-do, KR

72 Inventor/es: **Choi, Yang-Lim;**
Cho, Jung-Yon y
Sohn, Young-Chul

74 Agente: **Curell Suñol, Marcelino**

Aviso: En el plazo de nueve meses a contar desde la fecha de publicación en el Boletín europeo de patentes, de la mención de concesión de la patente europea, cualquier persona podrá oponerse ante la Oficina Europea de Patentes a la patente concedida. La oposición deberá formularse por escrito y estar motivada; sólo se considerará como formulada una vez que se haya realizado el pago de la tasa de oposición (art. 99.1 del Convenio sobre concesión de Patentes Europeas).

DESCRIPCIÓN

Aparato y procedimiento para comunicar el estado de funcionamiento de la gestión de derechos digitales.

5 La presente invención se refiere a la gestión de derechos digitales (DRM) y, más particularmente, a un aparato y a un procedimiento para comunicar el estado de funcionamiento de la gestión de derechos digitales de un dispositivo de control, a un punto de control de una red doméstica.

10 Recientemente, los sistemas de redes domésticas han suscitado la atención de un número cada vez mayor de personas. Las redes domésticas se forman con dispositivos que reproducen un contenido (una película, una canción o un software de videojuego) y dispositivos que gestionan los dispositivos reproductores de contenido. En dichas redes, la gestión de derechos digitales es garantizada por dichos dispositivos.

15 La gestión de derechos digitales incluye una función para gestionar los derechos sobre dispositivos que pertenecen a una red doméstica, y una función para gestionar los derechos sobre el contenido reproducible en una red doméstica predeterminada. La gestión de derechos digitales es realizada por un programa de aplicación instalado en un dispositivo perteneciente a una red doméstica. Entre los programas de aplicación de gestión de derechos digitales utilizados actualmente, cabe mencionar SmartRight propuesto por Thomson, Open Conditional Content Access Management (OCCAM) propuesto por Cisco Systems, xCP (extensible content protection) Cluster Protocol propuesto por IBM y
20 Digital Transmisión Content Protection (DTCP) propuesto por Digital Transmisión License Administrator (DTLA).

25 En un sistema de gestión de derechos digitales corriente, los dispositivos que pertenecen a una red doméstica se clasifican en dispositivos maestros y dispositivos esclavos. Un dispositivo maestro es un dispositivo que concede, cambia o revoca derechos digitales sobre otros dispositivos, y establece, cambia y revoca derechos digitales sobre el contenido existente en la red doméstica. Un dispositivo esclavo es un dispositivo que proporciona o reproduce un contenido, de acuerdo con los derechos digitales concedidos por el dispositivo maestro. Los dispositivos esclavos se subdividen en reproductores de medios que decodifican y reproducen un contenido, y en generadores de medios que proporcionan un contenido a los reproductores de medios. La función realizada por el programa de aplicación DRM es lo que determina si un dispositivo es un dispositivo maestro o un dispositivo esclavo.

30 Mientras tanto, en los sistemas de redes domésticas recientes, se utiliza un protocolo uPnP (universal plug and play) para las comunicaciones entre el dispositivo maestro y los dispositivos esclavos. En la tecnología uPnP, es posible reconocer automáticamente si un dispositivo que forma parte de la red doméstica se ha conectado a la red doméstica o se ha desconectado de la misma y, por lo tanto, es posible conceder o revocar automáticamente el estado, como elemento de la red doméstica.
35

La Figura 1 es un diagrama que representa una red doméstica según un protocolo uPnP.

40 La red doméstica según el protocolo uPnP comprende un dispositivo de control (CD) y un punto de control (CP).

El CP 10 busca los CD 20, 30 y 40 por la red y, a través de la recepción de los mensajes de aviso generados tras la conexión o desconexión de un dispositivo de la red doméstica, reconoce que un CD se acaba de conectar a la red doméstica. Asimismo, el CP 10 recibe un mensaje de descripción de cada CD y unos mensajes de eventos según las acciones con los CD. Cada acción es definida mediante un lenguaje de etiquetado (por ejemplo, el lenguaje de etiquetado extensible o XML).
45

Cuando uno de los CD 20, 30 y 40 se conecta a la red doméstica o se desconecta de la red doméstica, éste envía un mensaje de aviso al CP 10 y envía un mensaje que confirma si el CD existe o no en la red doméstica dentro de un período predeterminado. Asimismo, los CD 20, 30 y 40 responden a una diversidad de peticiones transmitidas por el CP 10, de conformidad con el protocolo uPnP. Los CD 20, 30 y 40 pueden ser cualesquiera de los generadores y reproductores de medios de la red doméstica. En la Figura 1, las trayectorias 12, 14 y 16 indican las transmisiones de mensajes y las respuestas a mensajes que han tenido lugar entre el CP 10 y los CD 20, 30 y 40, y las trayectorias 22, 32 indican la transmisión y la recepción de contenidos entre los CD 20, 30 y 40.
50

55 La Figura 2 es un diagrama que representa una estructura en la cual se produce la transmisión de un contenido entre un CP y varios CD durante la gestión de derechos digitales (DRM), mediante el uPnP.

El CP 210 comprende un módulo uPnP 212 que transmite mensajes a los CD y recibe desde éstos las respuestas a los mensajes de conformidad con el protocolo uPnP, y una interfaz de usuario 214 que recibe una entrada del usuario para la transmisión de mensajes y proporciona al usuario los resultados de las respuestas a los mensajes. Generalmente, el CP 210 es un dispositivo de control remoto o un asistente personal digital (PDA) que presenta una pantalla de presentación visual. En el aspecto de la reproducción de contenidos, el CP 210 transfiere las órdenes de búsqueda y reproducción de contenidos del usuario a los CD, según el protocolo uPnP, y recibe las respuestas a las órdenes desde los CD.
60

65 Los CD se subdividen en reproductores de medios y generadores de medios, dependiendo de si reproducen o proporcionan contenidos.

ES 2 273 314 T3

El generador de medios 220 comprende un módulo uPnP 222 que avisa al CP 210 de su presencia a través de un mensaje de aviso, comunicándose con el módulo uPnP 212 del CP 210; un módulo DRM 224 que lleva a cabo la gestión de derechos digitales y proporciona los contenidos a los CD autorizados; y una BD (base de datos) de contenidos 226 en la que se almacenan los contenidos.

El reproductor de medios 230 comprende un módulo uPnP 232 que avisa al CP 210 de su presencia a través de un mensaje de aviso, comunicándose con el módulo uPnP 212 del CP 210; un módulo DRM 234, que lleva a cabo la gestión de derechos digitales y recibe los contenidos autorizados desde un generador de medios; y una unidad de reproducción de contenidos 236 que decodifica y reproduce los contenidos recibidos.

No obstante, como se representa en la Figura 2, mientras se comunican directamente entre sí, el módulo DRM 224 del generador de medios 220 y el módulo DRM 234 del reproductor de medios 230 realizan la gestión de derechos digitales. En consecuencia, el CP 210 sólo reconoce los mensajes de error que se generan de acuerdo con el protocolo uPnP. Es decir, el CP no puede saber qué operación del procedimiento DRM está realizando el generador de medios 220 o el reproductor de medios 230, o si el procedimiento se está realizando de forma satisfactoria o no.

En la implementación convencional de la Figura 2, se plantea el problema de que el usuario no puede reconocer el estado de funcionamiento del módulo DRM. Esto es debido a que la comunicación entre el CP y los CD se realiza a través del módulo uPnP, pero la comunicación entre el generador de medios y el reproductor de medios se realiza directamente a través del módulo DRM. Este problema causa un problema adicional, en la medida en que el usuario no puede enfrentarse fácilmente a los errores que se producen durante el procedimiento DRM.

En el documento WO 2004/017664, se da a conocer un agente de gestión de derechos digitales (DRM) implementado en un módulo de identidad resistente a intrusiones, adaptado para cooperar con el sistema del cliente (por ejemplo, un teléfono móvil o un sistema informático). El agente DRM se implementa con funciones que permiten la utilización, es decir, la reproducción o la ejecución, del contenido digital protegido proporcionado por un proveedor de contenidos al sistema del cliente. Este documento constituye la parte precaracterizadora de las reivindicaciones adjuntas.

Las formas de realización ilustrativas y no limitativas de la presente invención pretenden abordar y resolver los inconvenientes anteriores y otros inconvenientes no descritos. No obstante, debe observarse que la presente invención no es necesaria para superar los inconvenientes descritos anteriormente, y que es posible que alguna forma de realización ilustrativa y no limitativa de la presente invención no resuelva ninguno de los problemas descritos.

Según la presente invención, se proporciona un aparato y un procedimiento según las reivindicaciones adjuntas. Las características preferidas de la presente invención se pondrán de manifiesto a partir de las reivindicaciones subordinadas y la descripción proporcionada a continuación.

En general, la presente invención proporciona un procedimiento para comunicar el estado de funcionamiento de la gestión de derechos digitales (DRM), por medio del cual el usuario puede reconocer el estado de funcionamiento del procedimiento DRM en un sistema DRM en el que se utiliza el protocolo uPnP (universal plug and play).

Según un aspecto de la presente invención, se proporciona un aparato para comunicar el estado de funcionamiento de la gestión de derechos digitales DRM de un dispositivo de control a un punto de control de una red doméstica, que está constituida por lo menos por un dispositivo de control y un punto de control, comprendiendo dicho aparato: un módulo DRM que realiza la DRM; caracterizado porque comprende: una unidad de generación de variables de estado dispuesta para recibir, desde el módulo DRM, información de estado de funcionamiento DRM de un procedimiento DRM que está siendo realizado actualmente, y generar variables de estado DRM basándose en la información de estado DRM recibida; y un módulo uPnP (universal plug and play) que está dispuesto para transmitir las variables de estado generadas por la unidad de generación de variables de estado al punto de control, mediante el protocolo uPnP.

La información de estado DRM puede indicar que la autenticación realizada por el módulo DRM ha empezado, que está en curso, que ha fallado o que se ha realizado con éxito. Asimismo, la información de estado DRM puede indicar que el procesamiento de clave realizado por el módulo DRM está en curso, ha fallado o ha terminado con éxito.

Entonces, cuando el dispositivo de control es un generador de medios, la información de estado DRM puede generarse siempre que se proporcione un contenido del generador de medios a otro dispositivo de control, y cuando el dispositivo de control es un reproductor de medios, la información de estado DRM puede generarse siempre que se introduzca un contenido del reproductor de medios en el reproductor de medios o siempre que se reproduzca dicho contenido.

La unidad de generación de variables de estado puede generar además: una variable de estado no autenticada que indica que se ha encendido el dispositivo de control que incluye el módulo DRM; una variable de estado de funcionamiento normal que indica que el módulo DRM está funcionando con normalidad; una variable de estado de autenticación que indica que el módulo DRM está realizando una operación de autenticación y una variable de estado de fallo de autenticación que indica que la autenticación realizada por el módulo DRM ha fallado.

La unidad de generación de variables de estado puede generar además: una variable de estado de funcionamiento normal que indica que el módulo DRM está funcionando con normalidad; una variable de estado de procesamiento de clave que indica que el módulo DRM está realizando una operación de procesamiento de clave y una variable de estado de fallo de procesamiento de clave que indica que la operación de procesamiento de clave realizada por el DRM ha fallado.

El aparato puede incluir también una unidad de almacenamiento de variables de estado en la que se almacenan las variables de estado y en la que, en respuesta a una petición de búsqueda de una variable de estado del punto de control, el módulo uPnP realiza la búsqueda de una variable de estado almacenada, de conformidad con el protocolo uPnP, y transmite la variable de estado al punto de control.

Según otro aspecto de la presente invención, se proporciona un procedimiento para comunicar el estado de funcionamiento de la gestión de derechos digitales DRM de un dispositivo de control a un punto de control de una red doméstica, formada por el dispositivo de control y el punto de control, comprendiendo el procedimiento:

realizar la DRM;
caracterizada porque comprende:
generar la información de estado DRM que determina la operación DRM que se está realizando actualmente;
generar una variable de estado DRM basándose en la información de estado DRM y
transmitir la variable de estado DRM generada al punto de control (360) mediante el protocolo uPnP (universal plug and play).

Los aspectos anteriores y otros aspectos de la presente invención resultarán más evidentes a partir de la siguiente descripción detallada de los ejemplos de las formas de realización de ésta, con referencia a los dibujos adjuntos, en los que:

la Figura 1 es un diagrama que representa una red doméstica según un protocolo uPnP (universal plug and play);

la Figura 2 es un diagrama que representa una estructura en la que la transmisión de contenidos entre un punto de control (CP) y un dispositivo de control (CD) se realiza durante la gestión de derechos digitales (DRM), utilizando el uPnP;

la Figura 3 es un diagrama que representa las estructuras internas de un CP y un CD según un ejemplo de forma de realización de la presente invención;

la Figura 4 es un diagrama que representa la transición de las variables de estado según un ejemplo de forma de realización de la presente invención;

la Figura 5 es un diagrama que representa la transición de variables de estado según otro ejemplo de forma de realización de la presente invención;

la Figura 6 es un diagrama que representa la transición de variables de estado según otro ejemplo de forma de realización de la presente invención; y

la Figura 7 es un diagrama que representa un procedimiento para comunicar una variable de estado de revocación de derechos a un CP según un ejemplo de forma de realización de la presente invención.

A continuación, se proporcionará información más detallada acerca de la presente invención, haciendo referencia a los dibujos adjuntos, en los que se representan ejemplos de formas de realización de la presente invención.

Con referencia al diagrama de la Figura 3, en el que se representan las estructuras internas de un CD y un CP, el CD 300 según un ejemplo de forma de realización de la presente invención incluye un módulo DRM 310, un módulo uPnP 320, una BD de contenidos 330, una unidad de generación de variables de estado 340 y una unidad de almacenamiento de variables de estado 350. El CD 300 de la Figura 3 es un generador de medios.

El módulo DRM 310 realiza la gestión de derechos digitales del CD 300 de la red doméstica a la cual pertenece el módulo DRM 310. La gestión de derechos digitales incluye: i) la gestión de los derechos del dispositivo, ii) la gestión de los derechos del contenido y iii) la gestión de la revocación de los derechos.

La gestión de derechos del dispositivo comprende una serie de operaciones que incluye: i) la cesión, el cambio y la revocación de la calificación de los dispositivos pertenecientes a la red doméstica, ii) la generación, el cambio y la terminación de una clave de dominio que sólo puede ser obtenida por los dispositivos que pertenecen a la red doméstica y iii) la confirmación de la calificación de los dispositivos de la red doméstica utilizando la clave de dominio.

ES 2 273 314 T3

La gestión de derechos del contenido comprende una serie de operaciones que incluye: i) la generación, el cambio y la terminación de la información de control de copia (por ejemplo, la frecuencia permitida o el permiso de copia o reproducción de un contenido predeterminado y ii) la generación de una clave de contenido utilizada para la encriptación de unos contenidos predeterminados.

La gestión de la revocación de los derechos comprende una serie de operaciones que incluye la determinación de si se ha realizado o no una copia ilegal de los dispositivos y la revocación de los derechos digitales de todos los dispositivos que presentan el identificador que determina que se ha realizado una copia ilegal del dispositivo.

La revocación de los derechos se realiza utilizando una lista de revocaciones que incluye el identificador de los dispositivos copiados ilegalmente, y utilizando además las tecnologías de certificados o firmas electrónicas.

Las trayectorias 312, 322, 332 y 372 de la Figura 3 representan las trayectorias de comunicación uPnP para realizar una operación de transferencia de contenido desde el CD 300 hasta otro dispositivo, mediante una entrada del usuario a través del CP 360.

El módulo DRM 310 viene determinado por el mecanismo de gestión de derechos digitales utilizado por el módulo DRM 310. Entre los mecanismos de gestión de derechos digitales, cabe citar: SmartRight propuesto por Thomson, Open Conditional Content Access Management (OCCAM) propuesto por Cisco Systems, xCP (extensible content protection) Cluster Protocol propuesto por IBM y Digital Transmission Content Protection (DTCP) propuesto por Digital Transmisión License Administrator (DTLA).

Además de estos programas de aplicación de gestión de derechos digitales, el módulo DRM de la presente invención indica todos los mecanismos que realizan i) la gestión de los derechos del dispositivo, ii) la gestión de los derechos del contenido y iii) la gestión de la revocación de los derechos. La DRM puede implementarse mediante hardware, así como mediante programas de aplicación.

El módulo uPnP 320 detecta automáticamente si el dispositivo se ha conectado a la red doméstica o si se ha desconectado de ésta mediante el protocolo uPnP, actualiza automáticamente la información sobre todos los dispositivos conectados y realiza las acciones de petición y respuesta entre el CD 300, es decir, el generador de medios y el reproductor de medios, y el CP 360.

Las trayectorias 342, 352, 354, 356, 358 y 374 de la Figura 3 indican las trayectorias para la generación y la comunicación de las variables de estado DRM.

La unidad de generación de variables de estado 340 recibe información de estado DRM 342 desde el módulo DRM 310 y, mediante la información de estado DRM recibida 342, genera una variable de estado 352. La información de estado DRM varía según el tipo de mecanismo DRM utilizado por el módulo DRM. Puesto que todos los mecanismos DRM incluyen generalmente una operación de autenticación, una operación de procesamiento de clave y una operación de revocación, la información de estado DRM indica si la operación de autenticación realizada por el módulo DRM ha empezado o no, si la autenticación se ha realizado con éxito o no, si la operación de procesamiento de clave ha empezado o no y si la operación de procesamiento de clave ha fallado o no.

En la unidad de almacenamiento de variables de estado 350, se almacenan las variables de estado de funcionamiento. El módulo uPnP 370 del CP 360 transmite una petición de variable de estado al módulo uPnP 320 del CD 300 en un momento o período de tiempo predeterminado. El módulo uPnP 320 del CD 300 que recibe la petición de variable de estado 352 extrae la variable de estado actual almacenada en la unidad de almacenamiento de variables de estado 350 y, a continuación, transmite una respuesta 358 que contiene la variable de estado actual al módulo uPnP 370 del CP 360. La variable de estado actual transmitida 374 se presenta al usuario a través de la IU (interfaz de usuario) 380.

Con referencia a las Figuras 4 a 7, se describirá, a continuación, el procedimiento de transición de las variables de estado según cada mecanismo DRM.

La Figura 4 es un diagrama que representa la estructura de transición de las variables de estado según un ejemplo de forma de realización de la presente invención.

Las variables de estado de funcionamiento de la Figura 4 incluyen: Not_authenticated (no autenticado), Authenticating (Autenticación), Authentication_failed (fallo de autenticación), Processing_content_key (procesamiento de clave de contenido), Content_key_process_failure (fallo de procesamiento de clave de contenido), Normal_operation (OK) (operación normal, bien) y Unknown (Desconocido).

En la Figura 4, cada flecha indica la información de estado DRM 342 generada por el módulo DRM 310 según el estado de funcionamiento del módulo DRM 310, y cada bloque indica una variable de estado de funcionamiento 352.

Al encenderse el CD 300, se inicializa el módulo DRM 310. La unidad de generación de variables de estado 340 recibe la información del fin de la inicialización del módulo DRM 310 como información de estado DRM, genera la variable de estado "Not_authenticated" y la almacena en la unidad de almacenamiento de variables de estado 350.

ES 2 273 314 T3

El usuario introduce una orden de reproducción para un contenido predeterminado a través de la IU 380, a continuación dicha orden es transferida al módulo DRM (310) a través del módulo uPnP 370 del CP 360 y el módulo uPnP 320 del CD 300 y, finalmente, el módulo DRM 310 lleva a cabo la autenticación entre el CP 360 y el CD 300 según un mecanismo DRM predeterminado.

Si se inicia esta operación de autenticación, el módulo DRM 310 genera información de estado DRM 342 que indica el principio de la autenticación y la transmite a la unidad de generación de variables de estado 340. La unidad de generación de variables de estado 340 recibe la información de estado DRM 342 que indica el inicio de la autenticación y, a continuación, induce a la variable de estado “Not_authenticated” de la unidad de almacenamiento de variables de estado 350 a hacer la transición a “Authenticating”. La operación de transición de la variable de estado conlleva la operación de actualización de la variable de estado almacenada en la unidad de almacenamiento de variables de estado 350 con otra variable de estado.

De la misma manera, el módulo DRM 310 genera información de estado DRM con respecto a la operación que realiza el propio módulo DRM 310, siendo recibida dicha información de estado DRM por la unidad de generación de variables de estado 340 desde el módulo DRM 310 y, a continuación, según la estructura representada en la Figura 4, la variable de estado de la unidad de almacenamiento de variables de estado 350 se actualiza mediante la variable de estado correspondiente al bloque indicado en cada información de estado DRM.

En la Figura 4, la variable de estado “Normal_operation (OK)” indica que tanto la operación de procesamiento de clave como la operación de autenticación se han realizado con éxito.

La variable de estado “Unknown” es una variable de estado generada por la unidad de generación de variables de estado cuando la información de estado DRM 342 no es ninguno de los otros tipos de información de estado DRM representados en la Figura 4.

En la Figura 4, se representa la estructura de las variables de estado DRM cuando el mecanismo DRM es el DTCP (Digital Transmission Content Protection). Según el mecanismo DTCP, la autenticación de un CD se aplica a los respectivos contenidos. En consecuencia, con respecto al mecanismo DTCP, si la operación de autenticación de un dispositivo ha finalizado, se genera de inmediato la variable de estado “Key_processing” y no se genera ninguna otra variable de estado adicional.

La Figura 5 es un diagrama que representa la estructura de transición de variables de estado según otro ejemplo de forma de realización de la presente invención.

La estructura de transición de estados de la Figura 5 representa un caso en el que la operación de autenticación y la operación de procesamiento de clave realizadas por módulo DRM (310) tienen lugar por separado.

Es decir, si la unidad de generación de variables de estado 340 recibe, durante el estado “Authenticating”, información de estado DRM que indica que la autenticación se ha realizado con éxito, la variable de estado cambia a “Normal_operation (OK)”. Dicho de otro modo, aunque la operación de autenticación se haya realizado con éxito, la variable de estado se actualiza con la variable de estado “Normal_operation (OK)”, a diferencia de lo que sucede en la Figura 4. En consecuencia, a menos que el usuario introduzca una orden de reproducción de un contenido predeterminado, la variable “Normal_operation (OK)” se mantiene hasta que la unidad de generación de variables de estado 340 recibe información de estado DRM 342 que indica que la autenticación ha finalizado.

Por consiguiente, la estructura de transición de estados de la Figura 5 es adecuada para un mecanismo DRM del módulo DRM 310, en el que las operaciones de autenticación se realizan por separado de las operaciones de procesamiento de clave; es decir, en el que las operaciones de autenticación se realizan para unos dispositivos predeterminados, mientras que las operaciones de procesamiento de clave se realizan para cada contenido, independientemente de los dispositivos.

La Figura 6 es un diagrama que representa la estructura de transición de las variables de estado según otro ejemplo de forma de realización de la presente invención.

La estructura de transición estados de la Figura 6 es igual a la de la Figura 5, excepto por la variable de estado “Revocated” (revocados). La variable de estado “Revocated” se genera cuando, durante la operación de autenticación de un dispositivo, se determina que éste ha sido copiado ilegalmente. En consecuencia, la estructura de transición de estados de la Figura 6 es adecuada para un mecanismo DRM del módulo DRM 310 que realiza la función de revocación.

En otra forma de realización de la presente invención, a diferencia de la representada en la Figura 3, la variable de estado “Revocated” puede ser transferida al CP mediante un procedimiento distinto al de respuesta a una petición de variable de estado. Esta posibilidad se describirá a continuación.

La Figura 7 es un diagrama que representa un procedimiento para comunicar la variable de estado de revocación de derechos a un CP según un ejemplo de forma de realización de la presente invención.

ES 2 273 314 T3

En la forma de realización de la Figura 7, la variable de estado “Revocated” se transfiere del CD al CP a través de la orden “get_protocol info” (obtención de información de protocolo) que es una de las acciones uPnP.

En primer lugar, en la operación ①, el CP transfiere la orden “get_protocol info” al CD según el protocolo uPnP. El CD incluye tanto un generador de medios (MS) como un reproductor de medios (MR). La transferencia de la orden “get_protocol info” tiene lugar entre el módulo uPnP del CP y el módulo uPnP del CD.

En la operación ②, cada CD, es decir, el generador de medios (MS) y el reproductor de medios (MR), transfiere al CP una respuesta a la orden “get_protocol info”. Esta respuesta contiene la variable de estado “Revocated” que indica si el generador de medios o el reproductor de medios han sido copiados ilegalmente o no. La variable de estado “Revocated” es generada por la unidad de generación de variables de estado del CD.

En la operación ③, el CP transmite una orden de búsqueda y consulta de un contenido predeterminado al generador de medios y, en respuesta a la orden, el generador de medios transmite, en la operación ④, información de contenido que contiene un identificador de indica el contenido predeterminado.

En las operaciones ⑤ a ⑧, se realizan las órdenes de direccionamiento y reproducción para el correspondiente contenido entre el CP y el reproductor de medios y, de ese modo, se reproduce dicho contenido.

En las operaciones ⑤ y ⑥, el reproductor de medios (MR) recibe información sobre el generador de medios en el que se almacena el contenido y la ubicación del contenido a través de la orden SET_AVTURI del CP y, en las operaciones ⑦ y ⑧, recibe el correspondiente contenido desde el generador de medios (MS) a través de la orden “Play” (reproducción) del CP y reproduce el contenido.

En la Figura 7, las operaciones ① y ② pueden realizarse después de las operaciones ③ y ④. En este caso, una vez efectuada la búsqueda y la consulta de un contenido predeterminado, se transmite la orden “get_protocol info” desde el CP hasta el CD.

Mientras tanto, el procedimiento para comunicar el estado de funcionamiento de la gestión de derechos digitales según la presente invención puede grabarse como un programa informático. Los códigos y los segmentos de código que forman el programa pueden ser fácilmente deducidos por los programadores informáticos dentro del campo de la presente invención. Además, el almacenamiento del programa en unos medios legibles por ordenador y su lectura y ejecución por un ordenador permiten implementar la comunicación del estado de la gestión de derechos digitales. Los medios legibles por ordenador incluyen los medios de almacenamiento magnético, los medios de registro óptico y los medios de ondas portadoras.

Según la presente invención descrita en la presente memoria, un punto de control que presenta una interfaz de usuario en una red doméstica está dispuesto para permitir la presentación ante el usuario del estado de funcionamiento de la gestión de derechos digitales, que es realizada por el dispositivo de control, de tal forma que el usuario pueda ocuparse sin dificultad de los estados de error de la red doméstica.

Aunque se han representado y descrito algunas formas de realización preferidas, los expertos en la materia apreciarán que es posible realizar diversos cambios y modificaciones en éstas sin apartarse del alcance de la presente invención, definido en las reivindicaciones adjuntas.

Todas las características dadas a conocer en la presente memoria (incluidas las reivindicaciones adjuntas, la descripción y los dibujos), o todas las etapas de los procedimientos o procesos dados a conocer, pueden unirse en cualquier combinación, excepto en combinaciones en las que por lo menos algunas de dichas características o etapas son mutuamente exclusivas.

Cada característica dada a conocer en la presente memoria (incluidas las reivindicaciones adjuntas, la descripción y los dibujos) puede ser sustituida por una característica alternativa que desempeña la misma función o una función equivalente o similar, a menos que se indique explícitamente lo contrario. Por lo tanto, a menos que se indique explícitamente lo contrario, cada una de las características dadas a conocer sólo representa un ejemplo de una serie genérica de características equivalentes o similares.

La presente invención no se restringe a los detalles de las formas de realización anteriores. La presente invención abarca cualquier característica nueva, o cualquier combinación nueva de características, dada a conocer en la presente memoria (incluidas las reivindicaciones adjuntas, la descripción y los dibujos), o cualquier etapa nueva, o cualquier combinación nueva de etapas, de cualquier procedimiento o proceso dado a conocer.

REIVINDICACIONES

5 1. Aparato para comunicar el estado de funcionamiento de la gestión de derechos digitales DRM de un dispositivo de control (300) a un punto de control (360) en una red doméstica, que está constituida por lo menos por un dispositivo de control (300) y un punto de control (360), comprendiendo dicho aparato:

un módulo DRM (310) que realiza la DRM;

10 **caracterizado** porque comprende:

una unidad de generación de variables de estado (340) dispuesta para recibir, desde el módulo DRM (310), información de estado de funcionamiento DRM de un procedimiento DRM que está siendo realizado actualmente, y generar variables de estado DRM basándose en la información de estado DRM recibida; y

15 un módulo uPnP (universal plug and play) (320) que está dispuesto para transmitir las variables de estado generadas por la unidad de generación de variables de estado (340) al punto de control (360), mediante el protocolo uPnP.

20 2. Aparato según la reivindicación 1, en el que la información de estado DRM proporciona por lo menos una de las siguientes indicaciones sobre la autenticación realizada por el módulo DRM (310): el inicio de la autenticación, la ejecución de la autenticación, el fallo de la autenticación o el éxito de la autenticación.

25 3. Aparato según la reivindicación 1 ó 2, en el que la información de estado DRM proporciona por lo menos una de las siguientes indicaciones sobre el procesamiento de clave realizado por el módulo DRM (310): la ejecución del procesamiento de clave, el fallo del procesamiento de clave o el éxito del procesamiento de clave.

30 4. Aparato según la reivindicación 2, en el que, cuando el dispositivo de control (300) es un generador de medios, la unidad de generación de variables de estado (340) está dispuesta para generar la información de estado DRM siempre que se proporcione el contenido del generador de medios a otro dispositivo de control (300) y, cuando el dispositivo de control (300) es un reproductor de medios, la unidad de generación de variables de estado (340) está dispuesta para generar la información de estado DRM siempre que se introduzca el contenido del reproductor de medios en el reproductor de medios o siempre que se reproduzca dicho contenido.

35 5. Aparato según cualquiera de las reivindicaciones anteriores, en el que el módulo uPnP (universal plug and play) (320) está dispuesto para transmitir la información de estado DRM al punto de control (360), mediante el protocolo uPnP.

6. Aparato según la reivindicación 5, en el que la información de estado DRM indica si los derechos de un dispositivo de red doméstica en el que está instalado el módulo DRM (310) han sido revocados o no.

40 7. Aparato según cualquiera de las reivindicaciones anteriores, en el que la unidad de generación de variables de estado (340) está dispuesta para generar:

45 una variable de estado no autenticada que indica que por lo menos un dispositivo de control (300) que incluye el módulo DRM (310) está encendido;

una variable de estado de funcionamiento normal que indica que el módulo DRM (310) está funcionando con normalidad;

50 una variable de estado de autenticación que indica que el módulo DRM (310) está realizando una operación de autenticación; y

una variable de estado de fallo de autenticación que indica que un resultado de la autenticación realizada por el módulo DRM (310) ha fallado.

55 8. Aparato según la reivindicación 7, en el que, si la información de estado DRM indica que el módulo DRM (310) ha iniciado la autenticación, la unidad de generación de variables de estado (340) hace que la variable de estado no autenticada sea cambiada por la variable de estado de autenticación.

60 9. Aparato según la reivindicación 7 u 8, en el que, si la información de estado DRM indica que la autenticación realizada por el módulo DRM (310) ha sido llevada a cabo con éxito, la unidad de generación de variables de estado (340) hace que la variable de estado de autenticación sea cambiada por la variable de estado de funcionamiento normal, y si la información de estado DRM indica que la autenticación realizada por el módulo DRM (310) ha fallado, la unidad de generación de variables de estado (340) hace que la variable de estado de autenticación sea cambiada por la variable de estado de fallo de autenticación.

65 10. Aparato según la reivindicación 7, 8 ó 9, en el que, cuando la información de estado DRM indica la condición de fin de la autenticación de por lo menos un dispositivo de control (300), la unidad de generación de variables de

estado (340) hace que la variable de estado de funcionamiento normal sea cambiada por la variable de estado no autenticada.

11. Aparato según la reivindicación 7, 8, 9 ó 10, en el que la unidad de generación de variables de estado (340) está dispuesta para generar además:

una variable de estado de procesamiento de clave que indica que el módulo DRM (310) está realizando una operación de procesamiento de clave; y

una variable de estado de fallo de procesamiento de clave que indica que la operación de procesamiento de clave realizada por el módulo DRM (310) ha fallado.

12. Aparato según la reivindicación 11, en el que, si la información de estado de funcionamiento DRM indica que la operación de autenticación realizada por el módulo DRM (310) ha sido llevada a cabo con éxito, la unidad de generación de variables de estado (340) hace que la variable de estado de autenticación sea cambiada por la variable de estado de procesamiento de clave, y si la información de estado DRM indica que la operación de autenticación realizada por el módulo DRM (310) ha fallado, la unidad de generación de variables de estado (340) hace que la variable de estado de procesamiento de clave sea cambiada por la variable de estado de fallo de autenticación.

13. Aparato según la reivindicación 11 ó 12, en el que, si la información de estado DRM indica que el módulo DRM (310) ha iniciado el procesamiento de clave, la unidad de generación de variables de estado (340) hace que la variable de estado de funcionamiento normal sea cambiada por la variable de estado de procesamiento de clave.

14. Aparato según la reivindicación 11, 12 ó 13, en el que, si la información de estado DRM indica que la operación de procesamiento de clave realizada por el módulo DRM (310) ha sido llevada a cabo con éxito, la unidad de generación de variables de estado (340) hace que la variable de estado de procesamiento de clave sea cambiada por la variable de estado de funcionamiento normal, y si la información de estado DRM indica que la operación de procesamiento de clave realizada por el módulo DRM (310) ha fallado, la unidad de generación de variables de estado (340) hace que la variable de estado de procesamiento de clave sea cambiada por la variable de estado de fallo de procesamiento de clave.

15. Aparato según cualquiera de las reivindicaciones anteriores, que comprende además:

una unidad de almacenamiento de variables de estado (350), en la que se almacenan las variables de estado y en la que, en respuesta a una petición de búsqueda de variable de estado del punto de control (360), el módulo uPnP (320) realiza una búsqueda de una variable de estado almacenada en la unidad de almacenamiento de variables de estado (350), según el protocolo uPnP, y transmite la variable de estado al punto de control (360).

16. Aparato según la reivindicación 15, en el que el módulo uPnP (universal plug and play) está dispuesto para transmitir la variable de estado a por lo menos un dispositivo de control (300) como respuesta a la orden "get_protocol info" emitida por el punto de control (360).

17. Procedimiento para comunicar el estado de funcionamiento de la gestión de derechos digitales (DRM) de un dispositivo de control (300) a un punto de control (360) de una red doméstica, formada por el dispositivo de control (300) y el punto de control (360), comprendiendo el procedimiento:

realizar la DRM;

caracterizada porque comprende:

generar la información de estado DRM que determina la operación DRM que se está realizando actualmente;

generar una variable de estado DRM basándose en la información de estado DRM; y

transmitir la variable de estado DRM generada al punto de control (360) mediante el protocolo uPnP (universal plug and play).

18. Procedimiento según la reivindicación 17, en el que la generación de la información de estado DRM tiene lugar mientras se realiza la DRM.

19. Procedimiento según las reivindicaciones 17 ó 18, en el que la información de estado DRM proporciona por lo menos una de las siguientes indicaciones sobre la autenticación realizada por el módulo DRM (310): el inicio de la autenticación, la ejecución de la autenticación, el fallo de la autenticación y el éxito de la autenticación.

20. Procedimiento según la reivindicación 19, en el que la información de estado DRM proporciona por lo menos una de las siguientes indicaciones sobre el procesamiento de clave realizado por el módulo DRM (310): la ejecución del procesamiento de clave, el fallo de procesamiento de clave y el éxito del procesamiento de clave.

ES 2 273 314 T3

21. Procedimiento según las reivindicaciones 19 ó 20, en el que, cuando el dispositivo de control (300) es un generador de medios, la información de estado DRM se genera siempre que se proporciona el contenido del generador de medios a otro dispositivo de control (300) y, cuando el dispositivo de control (300) es un reproductor de medios, la información de estado DRM se genera siempre que se introduce el contenido del reproductor de medios en el reproductor de medios o siempre que se reproduce dicho contenido.

22. Procedimiento según cualquiera de las reivindicaciones 17 a 21, en el que la información de estado DRM se transmite al punto de control (360), mediante el protocolo uPnP.

23. Procedimiento según la reivindicación 22, en el que la información de estado DRM indica si se ha revocado por lo menos un derecho del dispositivo de red doméstica en el cual está instalado el módulo DRM (310).

24. Procedimiento según cualquiera de las reivindicaciones 17 a 23, en el que la generación de la variable de estado DRM comprende la generación de:

una variable de estado no autenticada que indica que se ha encendido el dispositivo de control (300) que incluye un módulo DRM (310);

una variable de estado de funcionamiento normal que indica que el módulo DRM (310) funciona con normalidad;

una variable de estado de autenticación que indica que el módulo DRM (310) está realizando una operación de autenticación; y

una variable de estado de fallo de autenticación que indica que la autenticación realizada por el módulo DRM (310) ha fallado.

25. Procedimiento según la reivindicación 24, en el que, si la información de estado DRM indica que el módulo DRM (310) ha iniciado la autenticación, la generación de la variable de estado DRM comprende hacer que la variable de estado de no autenticación sea cambiada por la variable de estado de autenticación.

26. Procedimiento según la reivindicación 24 ó 25, en el que, si la información de estado DRM indica que la autenticación realizada por el módulo DRM (310) ha sido llevada a cabo con éxito, la generación de la variable de estado DRM comprende hacer que la variable de estado de autenticación sea cambiada por la variable de estado de funcionamiento normal, y si la información de estado DRM indica que la autenticación realizada por el módulo DRM (310) ha fallado, la generación de la variable de estado DRM comprende hacer que la variable de estado autenticada sea cambiada por la variable de estado de fallo de autenticación.

27. Procedimiento según la reivindicación 24, 25 ó 26, en el que, si la información de estado DRM indica una condición de fin de autenticación del dispositivo de control (300), la generación de la variable de estado DRM comprende hacer que la variable de estado de funcionamiento normal sea cambiada por la variable de estado no autenticada.

28. Procedimiento según cualquiera de las reivindicaciones 24 a 27, en el que la generación de la información de estado DRM comprende además la generación de:

una variable de estado de procesamiento de clave que indica que el módulo DRM (310) está realizando una operación de procesamiento de clave; y

una variable de estado de fallo de procesamiento de clave que indica que la operación de procesamiento de clave realizada por el módulo DRM (310) ha fallado.

29. Procedimiento según la reivindicación 28, en el que, si la información de estado DRM indica que la operación de autenticación realizada por el módulo DRM (310) ha sido llevada a cabo con éxito, la generación de la variable de estado DRM comprende hacer que la variable de estado de autenticación sea cambiada por la variable de estado de procesamiento de clave, y si la información de estado DRM indica que la operación de autenticación realizada por el módulo DRM (310) ha fallado, la generación de la variable de estado DRM comprende hacer que la variable de estado de procesamiento de clave sea cambiada por la variable de estado de fallo de autenticación.

30. Procedimiento según la reivindicación 28 ó 29, en el que, cuando la información de estado DRM indica que el módulo DRM (310) ha iniciado un procesamiento de clave, la generación de la variable de estado DRM comprende hacer que la variable de estado de funcionamiento normal sea cambiada por la variable de estado de procesamiento de clave.

31. Procedimiento según la reivindicación 28, 29 ó 30, en el que, si la información de estado DRM indica que la operación de procesamiento de clave realizada por el módulo DRM (310) ha sido llevada a cabo con éxito, la generación de la variable de estado DRM comprende hacer que la variable de estado de procesamiento de clave sea cambiada por la variable de estado de funcionamiento normal, y si la información de estado DRM indica que la operación de procesamiento de clave realizada por el módulo DRM (310) ha fallado, la generación de la variable de

ES 2 273 314 T3

estado DRM comprende hacer que la variable de estado de procesamiento de clave sea cambiada por la variable de estado de fallo de procesamiento de clave.

32. Procedimiento según cualquiera de las reivindicaciones 17 a 31, que comprende además:

5

almacenar la variable de estado DRM, en la que, durante la transmisión de la variable de estado DRM, la variable de estado DRM almacenada en la unidad de almacenamiento de variables de estado (350) se transmite al punto de control (360) en respuesta a una petición de búsqueda de variable de estado emitida por el punto de control (360).

10

33. Procedimiento según la reivindicación 32, en el que la variable de estado DRM se transmite al punto de control (360) en respuesta a la orden "get_protocol info" emitida por el punto de control (360).

15

20

25

30

35

40

45

50

55

60

65

FIG. 1 (TÉCNICA ANTERIOR)

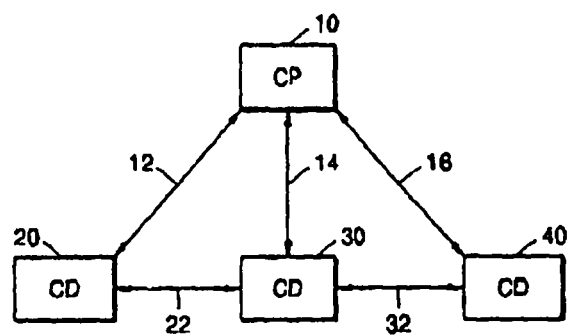


FIG. 2 (TÉCNICA ANTERIOR)

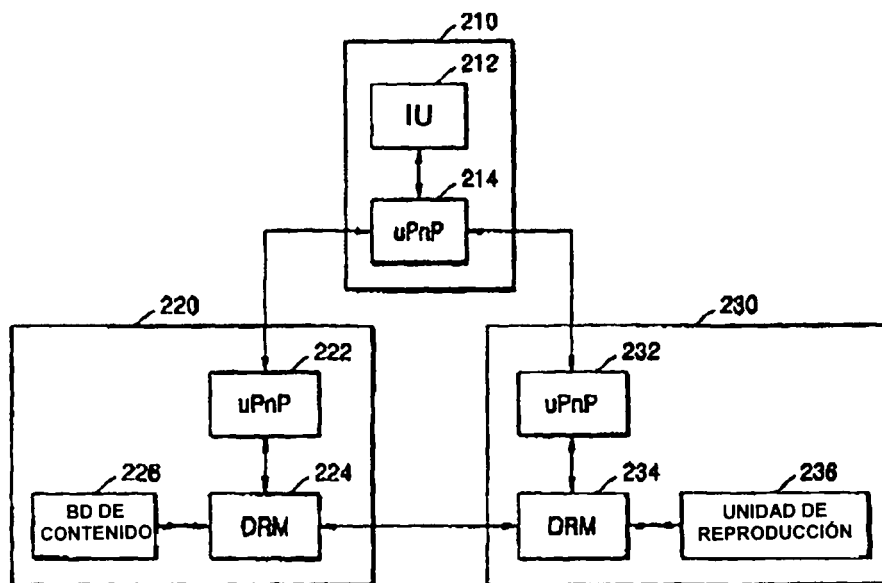


FIG. 3

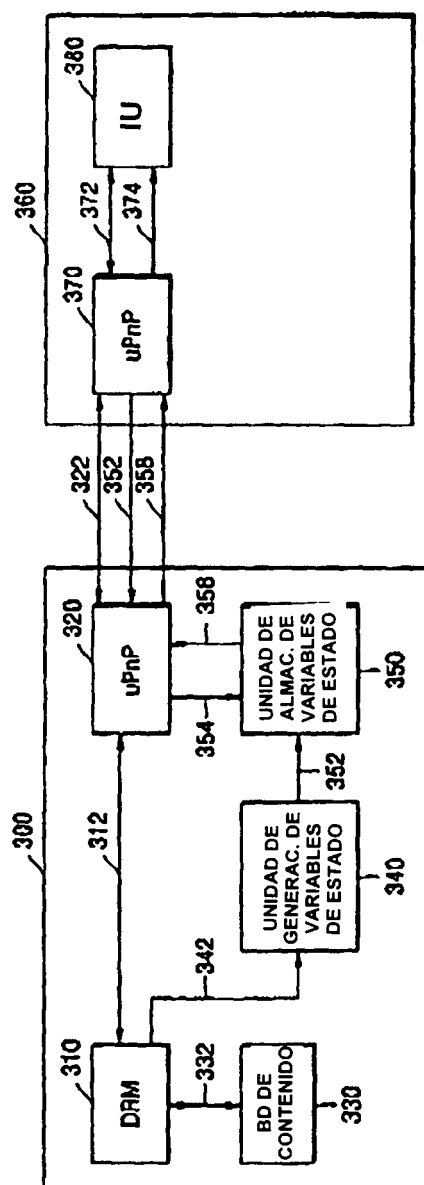


FIG. 4

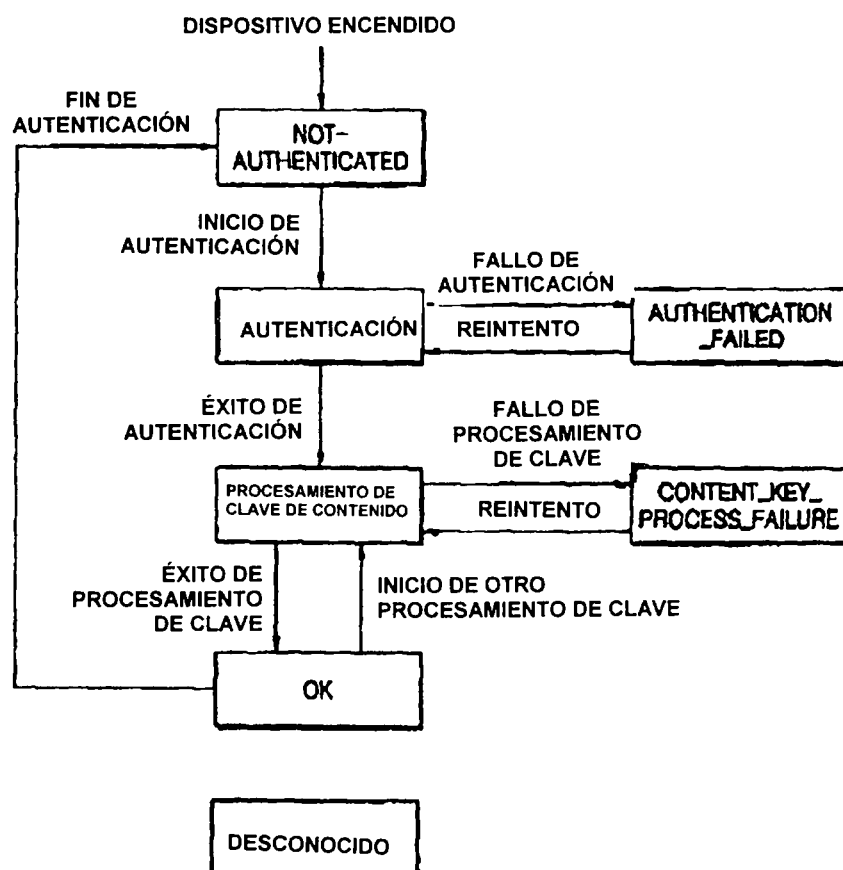


FIG. 5

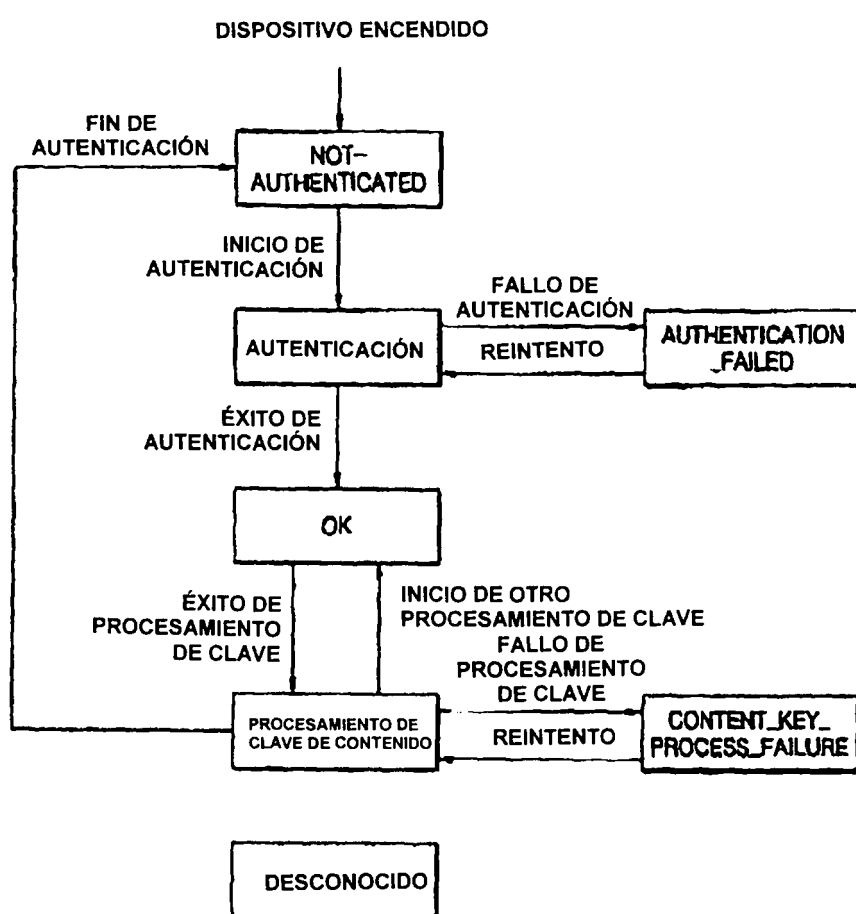


FIG. 6

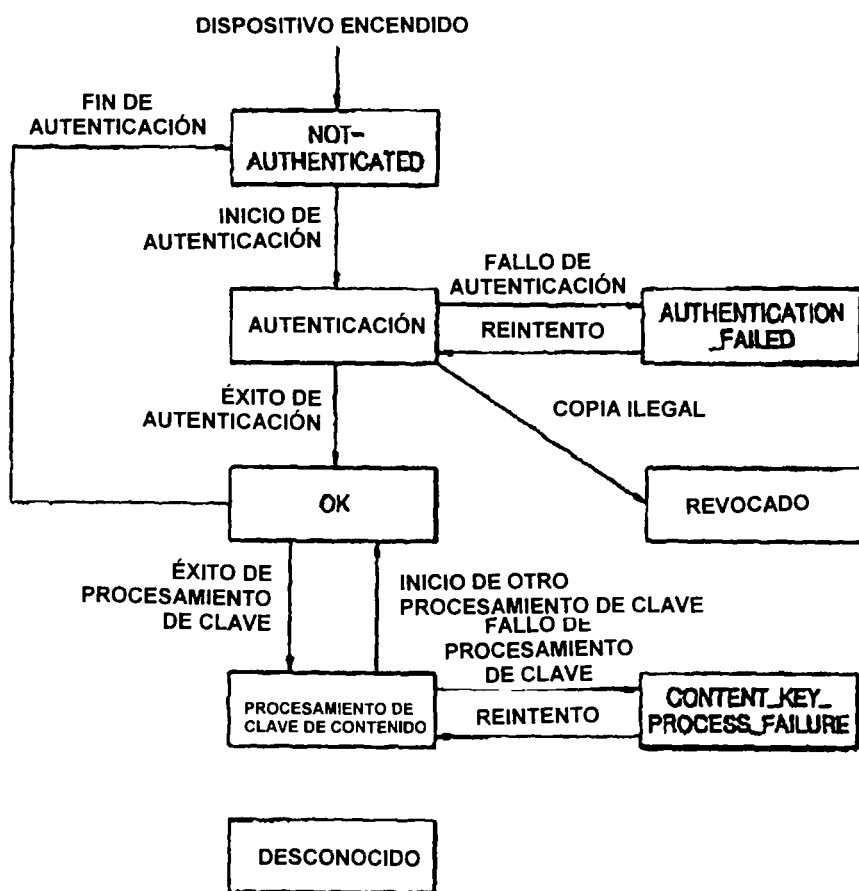


FIG. 7

