(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 356 089**

(51) Int. Cl.:
G06F 21/00 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **05739558 .4**
(96) Fecha de presentación : **11.05.2005**
(97) Número de publicación de la solicitud: **1751648**
(97) Fecha de publicación de la solicitud: **14.02.2007**

(54) Título: **Protección de la integridad de contenidos de difusión en continuo.**

(30) Prioridad: **12.05.2004 US 844063**

(45) Fecha de publicación de la mención BOPI:
04.04.2011

(45) Fecha de la publicación del folleto de la patente:
04.04.2011

(73) Titular/es: **NOKIA CORPORATION**
Keilalahdentie 4
02150 Espoo, FI

(72) Inventor/es: **Pippuri, Sami**

(74) Agente: **López Bravo, Joaquín Ramón**

DESCRIPCIÓN

ANTECEDENTES DE LA INVENCIÓN

Campo de la invención:

La invención se refiere a la gestión de derechos digitales en dispositivos electrónicos. En particular, la invención se refiere al establecimiento de secretos compartidos y a la protección de la integridad de los contenidos de difusión en continuo en dispositivos electrónicos aplicando una gestión de derechos digitales.

Descripción de la Técnica Relacionada:

Desde la introducción de las tecnologías de almacenamiento digital, la aplicación más eficaz de los derechos de autor se ha convertido en un problema. Especialmente, la emergencia de Internet como un canal de distribución ilícita de contenidos protegidos por derechos de autor ha creado una fuerte reivindicación de nuevas tecnologías en la protección de los derechos de autor. Una de estas tecnologías es la Gestión de Derechos Digitales (DRM). La DRM es un término común para los sistemas estándar y de propiedad, en los que a un elemento de contenido dado se le añade información que especifica los derechos de usuario asociados al mismo. El elemento de contenido puede ser, por ejemplo, una grabación de audio, vídeo, fotografía, programa de ordenador o simplemente un documento. Los derechos de los usuarios pueden comprender diversas reglas relacionadas con el uso del elemento de contenido. Por ejemplo, a un usuario se le puede dar un límite temporal durante el cual se le puede presentar el elemento de contenido, en otras palabras, se le puede suministrar al usuario. Otros ejemplos de normas relativas a la utilización de un elemento de contenido son el número de veces de escucha, las identidades del dispositivo permitidas y los derechos de visión parcial. La DRM requiere que el dispositivo de presentación y el software de presentación en el mismo no sean hostiles, es decir, participen en la aplicación de los derechos digitales. En el dispositivo de presentación suele haber un agente de DRM, o en otras palabras, un motor de DRM, que refuerza los derechos de DRM y protege los elementos de contenido contra la copia ilícita. Con el fin de evitar que un elemento de contenido protegido por DRM se pueda copiar, el elemento de contenido se puede encriptar mientras se encuentra en tránsito desde la red hasta el dispositivo de presentación y mientras está almacenado en el dispositivo de presentación exterior del motor de DRM, por ejemplo, en un disco duro. En el caso de contenidos en corriente continua, el contenido protegido con DRM no se descarga completamente al dispositivo de presentación antes de que sea presentado al usuario. Sin embargo, el contenido en corriente continua se puede proporcionar al dispositivo de presentación en un formato encriptado siempre que el dispositivo de presentación solicite iniciar la corriente continua del contenido. De manera similar, el contenido puede ser proporcionado a través del Protocolo de Internet (IP) de multidifusión en continuo de forma periódica. En cualquier caso, el contenido se proporciona en una forma encriptada.

Un estándar para la DRM es el basado en la especificación de DRM de la Open Mobile Alliance (OMA). El objetivo de la OMA DRM es permitir el consumo controlado de objetos de medios digitales permitiendo que los proveedores de contenido expresen los derechos de contenido. Los objetos de medios son los elementos de contenido tales como clips de audio, clips de video, imágenes, aplicaciones Java y documentos. Los elementos de contenido gobernados por derechos se conocen como activos. En la OMA DRM, los derechos de contenido se expresan como objetos en documento, es decir, documentos escritos utilizando un Lenguaje de Expresión de Derechos (REL). Con el fin de especificar los derechos que corresponden a un activo, el mismo se asocia a un objeto REL. La asociación entre un objeto REL y un activo puede ser especificada explícitamente mencionando el identificador del activo en el objeto REL o implícitamente proporcionando el objeto REL en un mismo mensaje, junto con el activo. En la OMA DRM hay tres procedimientos posibles para suministrar el contenido a un terminal y a un agente de DRM en el mismo. El contenido se suministra a un terminal móvil en los mensajes de DRM. En un mensaje de DRM hay un objeto de medio y un objeto de derecho opcional, es decir, un objeto REL. El primer procedimiento se denomina bloqueo hacia delante. En este procedimiento no hay ningún objeto REL asociado con el objeto de medio. El objeto de medio se envía en un mensaje de DRM, que no tiene objeto REL. Los derechos por defecto conocidos al MT se aplican para el objeto de medio. Por ejemplo, pueden prevenir una distribución adicional del objeto de medio a cualquier otro terminal. El segundo procedimiento se denomina entrega combinada. En la entrega combinada, un objeto de medio se envía junto con el objeto REL en un mensaje de DRM. En el tercer procedimiento, el objeto de medio y el objeto REL se proporcionan por separado. Pueden ser enviados por medio de diferentes transportes.

Un terminal móvil que aplica la DRM está equipado con un agente de DRM, es decir, un motor de DRM. Un objeto de medio o una corriente de medio, en otras palabras, una corriente de contenidos, se proporciona a través del motor de DRM para una aplicación de medio para su presentación al usuario. El motor de DRM desencripta el objeto de medio o la corriente de contenidos, si se ha encriptado para la protección. La encriptación opcional se ha realizado en una fuente de contenidos utilizando una encriptación que sólo puede ser desencriptada mediante una clave disponible por el motor de DRM. La clave típicamente es una clave simétrica de encriptado / desencriptado. Los terminales móviles

almacenan también al menos un objeto de regla. El objeto de regla es utilizado por el motor de DRM para comprobar los derechos de usuario que se refieren a un objeto de medio determinado. El motor de DRM verifica los derechos de usuario antes de hacer disponible el objeto de medio o la corriente, con la aplicación de medio para proporcionárselo al usuario.

Se hace referencia a continuación a la figura 1, que ilustra como se proporciona el medio de difusión en continuo y las claves de desencriptado de contenidos a un terminal que está equipado con un agente de DRM en la técnica anterior. En la figura 1 hay una entidad propietaria de contenido, que es, por ejemplo, un nodo propietario de contenido 110. Desde el nodo propietario del contenido 110, el contenido se proporciona a un número de servidores de difusión en continuo, tales como un servidor de difusión en continuo 112, que proporciona corrientes encriptadas a un número de clientes de contenido, tales como el cliente de contenido 114. La corriente del contenido actual se envía desde el servidor de difusión en continuo 112, por ejemplo, como una corriente de Protocolo en Momento Real. El Protocolo en Momento Real (RTP) se especifica en la Petición de Comentarios (RFC), número 1889 del Grupo de Trabajo de Ingeniería de Internet (IETF). Una corriente de RTP es transportada en paquetes de Protocolo de Internet (IP). La capa de transporte puede ser, por ejemplo, el Protocolo de Datagramas Universal (UDP). El cliente de contenido 114 solicita del servidor de difusión en continuo 112 el inicio de la corriente utilizando, por ejemplo, el Protocolo de Inicio de Sesión (SIP) especificado en el RFC 2543 o utilizando el Protocolo de Difusión en Continuo en Momento Real (RTSP) especificado en el RFC 2326. El cliente de contenido 114 se utiliza como un dispositivo de presentación de contenido, en el que el usuario puede ver y escuchar las presentaciones de difusión en continuo. Los derechos para visualizar una corriente de contenidos son obtenidos por el cliente de contenido 114 de un nodo emisor de derechos 116. Los derechos comprenden, al menos, una Clave de Encriptado de Contenido (CEK), que es utilizada por el motor de DRM para desencriptar el contenido de la difusión en continuo. Los derechos también pueden comprender la información asociada, por ejemplo, con el período de validez de los derechos. Debido al hecho de que la clave de encriptado de contenido es una clave simétrica, también se utiliza como una clave de desencriptado de contenido. La clave de encriptado de contenido se proporciona al motor de DRM en un formato, en el que se ha encriptado mediante una clave asimétrica asociada con el motor de DRM para el cliente de contenido receptor. La clave asimétrica puede ser, por ejemplo, una clave pública para el motor de DRM en el cliente de contenido 114. De esta forma sólo el motor de DRM para el cliente de contenido 114 que tiene en su posesión la clave privada podrá obtener la clave de encriptado de contenido.

En primer lugar, una corriente de contenidos está encriptada por el nodo propietario de contenido 110 con una CEK. Se debe hacer notar que el formato EKEY (DATA) denota un elemento de datos designado como DATA, encriptado utilizando KEY como clave de encriptado. La corriente de contenidos encriptada se entrega al servidor de corriente 112, por ejemplo, con la descarga de archivos en masa como se ilustra con la flecha 101. El nodo propietario de contenido proporciona la CEK 110 al nodo emisor de derechos 116 como se ilustra con la flecha 102. Cuando el cliente de contenido 114 desea iniciar la difusión en continuo de los contenidos, envía una solicitud de derecho, en la que se identifica a sí mismo, al nodo emisor de derechos 116, como se ilustra con la flecha 103. El cliente de contenido se designa como C en la figura 1. En respuesta a la solicitud de derecho, el nodo emisor de derechos 116 responde con la CEK, que ha sido encriptada utilizando la clave pública (C-PUB) del cliente de contenido 114. Esto se ilustra con la flecha 104. A continuación, el cliente de contenido 114 podrá empezar a recibir una corriente de contenidos que ha sido encriptada con la CEK del servidor de difusión en continuo 112. El inicio de la transmisión puede ser solicitado por separado por el servidor de difusión en continuo 112 o la corriente se puede proporcionar continuamente a través de multidifusión o difusión sin una solicitud separada del cliente de contenido 114.

Hay problemas en una arquitectura de difusión en continuo de contenidos como se ilustra en la figura 1. A pesar del hecho de que las corrientes de contenidos tales como la corriente ilustrada con la flecha 105 se encripta con la CEK, todavía es posible manipular la corriente de contenidos si un atacante situado entre el servidor de difusión en continuo 112 y el cliente de contenido 114 adquiere conocimientos que se refieren al efecto de manipulaciones de bits en la corriente de contenidos resultante que se proporciona al usuario. Estos conocimientos se puede obtener si la CEK no se cambia con suficiente frecuencia. Sin embargo, el cambio de la CEK requiere un protocolo adicional, lo que complica el funcionamiento del servidor de difusión en continuo 112, el cliente de contenido 114 y el emisor de derechos 116. Un ejemplo de un protocolo utilizado para este propósito es el la Introducción por Teclado de Internet Multimedia (MIKEY) especificado en el documento del IETF draft-ietf-ms-mikey-07.txt (en preparación).

SUMARIO DE LA INVENCIÓN:

La invención se refiere a un procedimiento para recibir al menos una corriente de contenidos. El procedimiento comprende: requerir información por medio de un dispositivo electrónico sobre la citada al menos una corriente de contenidos de un servidor de difusión en continuo; recibir información en el citado dispositivo electrónico en la al menos una corriente de contenidos, comprendiendo la información al menos un valor de inicialización y una clave de integridad maestra encriptada con una clave de contenido, desencriptar la citada clave de integridad maestra utilizando la citada clave de contenido en el citado

dispositivo electrónico; formar al menos una clave de integridad de sesión utilizando el citado al menos un valor de inicialización y la citada clave de integridad maestra en el citado dispositivo electrónico; recibir del citado servidor de difusión en continuo en el citado dispositivo electrónico la citada al menos una corriente de contenidos protegida en integridad, la citada corriente de contenidos protegida en integridad está protegida con la citada al menos una clave de integridad de sesión; verificar en el citado dispositivo electrónico la integridad de la citada al menos una corriente de contenidos protegida en integridad utilizando la citada al menos una clave de integridad de sesión, y desencriptar la citada al menos una corriente de contenidos protegida en integridad utilizando al menos en parte la clave de contenido.

La invención se refiere también a un procedimiento para proporcionar al menos una corriente de contenidos. El procedimiento comprende: recibir en un servidor de difusión en continuo una clave de integridad maestra, estando encriptada la clave de integridad maestra con una clave de contenido y al menos una corriente de contenidos encriptada desde un propietario de contenido; recibir una solicitud de información en al menos una corriente de contenidos desde un dispositivo electrónico; generar por el citado servidor de difusión en continuo al menos un valor de inicialización; enviar la información al dispositivo electrónico por el citado servidor de difusión en continuo como respuesta a la solicitud de información en al menos una corriente de contenidos, comprendiendo la información al menos un valor de inicialización y la clave de integridad maestra encriptada con una clave de contenido; formar al menos una clave de integridad de sesión en el citado servidor de difusión en continuo utilizando el citado al menos un valor de inicialización y la citada clave de integridad maestra; proteger en el citado servidor de difusión en continuo la integridad de al menos una corriente de contenidos utilizando la citada al menos una clave de integridad de sesión; y transmitir la al menos una corriente de contenidos protegidos utilizando al menos una clave de integridad de sesión, con el citado dispositivo electrónico.

La invención se refiere también a un dispositivo electrónico configurado para recibir al menos una corriente de contenidos, comprendiendo el dispositivo electrónico: un motor de gestión de derechos digitales configurado para almacenar una clave de contenido, para desencriptar una clave de integridad maestra encriptada utilizando la citada clave de contenidos, formar al menos una clave de integridad de sesión utilizando al menos un valor de inicialización y la citada clave de integridad maestra, y comprobar la integridad de al menos una corriente de contenidos protegida en integridad utilizando al menos una de las claves de integridad de sesión y una entidad de comunicación conectada comunicativamente con el motor de gestión de derechos digitales, estando configurada la citada entidad de comunicación para enviar al menos una solicitud de información en al menos una corriente de contenidos desde un servidor de difusión en continuo, para recibir información sobre al menos una corriente de contenidos que comprende al menos un valor de inicialización y la citada clave de integridad maestra encriptada, y para recibir del citado servidor de difusión en continuo la citada al menos una corriente de contenidos protegida en integridad.

La invención se refiere también a un nodo de red que comprende una entidad de difusión en continuo configurada para recibir al menos una clave de integridad maestra, la clave de la integridad maestra se encripta con una clave de contenido y al menos una corriente de contenidos encriptada, para recibir una solicitud de información sobre al menos una corriente de contenidos, para generar al menos un valor de inicialización, para enviar información como respuesta a la solicitud de información en al menos una corriente de contenidos, la información comprende el citado al menos un valor de inicialización y la clave de integridad maestra encriptada con una clave de contenido, para formar al menos una clave de integridad de sesión con el citado al menos un valor de inicialización y la citada clave de integridad maestra, para proteger la integridad de la citada al menos una corriente de contenidos utilizando la citada al menos una clave de integridad de sesión y transmitir la al menos una corriente de contenidos protegida en integridad utilizando la citada al menos una clave de integridad de sesión. La invención se refiere también a un programa de ordenador que comprende un código adaptado para realizar los pasos siguientes cuando se ejecuta en un sistema de tratamiento de datos: solicitar información por medio de un dispositivo electrónico en al menos una corriente de contenidos de un servidor de difusión en continuo; recibir información en el citado dispositivo electrónico en la al menos una corriente de contenidos, comprendiendo la información al menos un valor de inicialización y una clave de integridad maestra encriptada con una clave de contenido; desencriptar la citada clave de integridad maestra encriptada utilizando la citada clave de contenido en el citado dispositivo electrónico; formar al menos una clave de integridad de sesión utilizando el citado al menos un valor de inicialización y la citada clave de integridad maestra en el citado dispositivo electrónico; recibir del citado servidor de difusión en continuo en el citado dispositivo electrónico, la citada al menos una corriente de contenidos protegida en integridad, siendo protegida la citada al menos una corriente de contenidos protegida en integridad con la citada al menos una clave de integridad de sesión, verificar en el citado dispositivo electrónico la integridad de la citada al menos una corriente de contenidos protegida en integridad, utilizando la al menos una clave de integridad de sesión; y desencriptar la citada al menos una corriente de contenidos protegida en integridad utilizando, al menos en parte, la clave de contenido.

En una realización de la invención, una corriente de contenidos protegida en integridad significa una corriente de contenidos que comprende datos de verificación de la integridad formados utilizando una clave de integridad de sesión. Los datos de verificación de integridad puede ser, por ejemplo, una

secuencia de verificación de trama encriptada utilizando una clave de sesión. La secuencia de verificación de trama se ha obtenido calculando, por ejemplo, un código hash o un algoritmo de resumen de mensaje de una parte dada de la corriente de contenidos encriptados o no encriptados. Los datos de verificación de integridad también se pueden transmitir por separado. En una realización de la invención, el nodo de difusión en continuo es un servidor de difusión en continuo y el dispositivo electrónico es un cliente de contenido.

En una realización de la invención, se realiza una verificación de la integridad en el valor de inicialización y la clave de integridad maestra encriptada utilizando la clave de integridad de sesión en el dispositivo electrónico. El objetivo es evitar los ataques en los que el valor de inicialización y la clave de la integridad maestra encriptada son cambiados por un atacante situado entre el servidor de difusión en continuo y el dispositivo electrónico.

En una realización de la invención, la formación de la clave de integridad de sesión y la verificación de la integridad de la al menos una corriente de contenidos es efectuada por un motor de Gestión de Derechos Digitales (DRM), es decir, un medio de gestión de los derechos digitales, o en otras palabras, una entidad de DRM, asociada al dispositivo electrónico. El medio de gestión de derechos digitales puede ser implementado, por ejemplo, como software en el dispositivo electrónico, o utilizando un módulo de hardware y un posible software que lo acompaña. El término medio de gestión digital de derechos también puede significar, en general, las partes del software del dispositivo electrónico a cargo de las tareas relacionadas con la gestión digital de derechos, en otras palabras, no puede constituir una entidad lógica claramente separable en el software.

En una realización de la invención, la clave de contenido se proporciona a un nodo emisor de derechos desde el nodo propietario de contenido. La clave de contenido se encripta utilizando una clave pública asociada al dispositivo electrónico. La clave pública también se puede asociar a un usuario del dispositivo electrónico. Una solicitud de derechos de contenido es recibida identificando el dispositivo electrónico en el nodo emisor de derechos. Al menos la clave de contenido encriptada se envía al dispositivo electrónico como respuesta a la solicitud de derecho. La clave de contenido encriptada es desencriptada en el medio de gestión de derechos digitales en el dispositivo electrónico.

En una realización de la invención, la clave de integridad maestra encriptada se proporciona desde un nodo propietario de contenido a un nodo de difusión en continuo y la clave de integridad maestra de encriptado se almacena en el nodo de difusión en continuo.

En una realización de la invención, una corriente de paquetes IP comprende la al menos una corriente de contenidos.

En una realización de la invención, la clave de contenido es una clave simétrica utilizada en el encriptado simétrico. La clave de contenido es una clave de contenido de encriptado / desencriptado.

En una realización de la invención, el dispositivo electrónico es una estación móvil. La estación móvil puede ser una estación móvil del Sistema de Telecomunicaciones Móviles Universal (UMTS), una estación móvil del Sistema General de Radiocomunicaciones por Paquetes (GPRS) En una estación móvil, el usuario del dispositivo electrónico se identifica utilizando Módulos de Identidad de Abonado (SIM).

En una realización de la invención, el dispositivo electrónico es un terminal de red IP fija.

En una realización de la invención, los derechos que se asocian con objetos de medio y corrientes de contenidos están representados como objetos de regla o documentos, por ejemplo, expresados en formato OMA REL.

En una realización de la invención, el dispositivo electrónico es un dispositivo móvil, por ejemplo, un terminal de WLAN o un terminal dentro de un sistema de radio celular arbitrario. El terminal también puede ser una red de datos fija o un terminal de red de telecomunicaciones.

En una realización de la invención, el programa de ordenador se almacena en un soporte legible por ordenador. El medio legible por ordenador puede ser una tarjeta de memoria, disco magnético, disco óptico o cinta magnética retirables.

En una realización de la invención, el dispositivo electrónico es un dispositivo móvil, por ejemplo, un ordenador portátil, un ordenador de bolsillo, un terminal móvil o un asistente personal digital (PDA). En una realización de la invención, el dispositivo electrónico es un ordenador de escritorio o cualquier otro dispositivo informático.

Los beneficios de la invención se asocian con una mejor protección de la gestión de los derechos digitales. Con la invención, ahora es posible evitar la obstrucción de corrientes de contenidos en tránsito entre un nodo de difusión en continuo y un dispositivo electrónico. Un beneficio adicional es que las claves de protección de la integridad no están expuestas. No se permite que el servidor genere nuevas claves de encriptación, lo cual evita el peligro de ataques que utilizan el servidor y comprometen las

corrientes de contenidos de texto.

La invención evita el requisito de utilizar protocolos de seguridad adicionales. Por otra parte, la invención proporciona la autenticidad del contenido, que se verifica utilizando la clave de contenido que es conocida sólo por el propietario del contenido y el medio de gestión de los derechos digitales en el dispositivo electrónico. La invención proporciona autenticidad del origen de contenido utilizando clave de integridad maestra de confianza del servidor del nodo propietario de contenido. La invención también se puede aplicar para la protección de la integridad de corrientes de contenidos no encriptadas.

BREVE DESCRIPCIÓN DE LOS DIBUJOS:

Los dibujos que se acompañan, que se incluyen para proporcionar una mayor comprensión de la invención y que constituyen una parte de esta memoria descriptiva, ilustran las realizaciones de la invención y junto con la descripción, ayudan a explicar los principios de la invención. En los dibujos:

la figura 1 es un diagrama de bloques que ilustra la difusión en continuo protegida por DRM a un cliente de contenido en la técnica anterior;

la figura 2 es un diagrama de bloques que ilustra la difusión en continuo protegida por DRM y la integridad protegida a un cliente de contenido, de acuerdo con la invención;

la figura 3 es un diagrama de flujo que muestra una realización de un procedimiento de protección de la integridad de corrientes protegidas por DRM, de acuerdo con la invención; y

la figura 4 es un diagrama de bloques que ilustra un terminal móvil y un sistema para aplicar la protección de integridad a corrientes protegidas por DRM, de acuerdo con la invención.

DESCRIPCIÓN DETALLADA DE LAS REALIZACIONES:

A continuación se hará referencia en detalle a las realizaciones de la presente invención, ejemplos de las cuales se ilustran en los dibujos adjuntos.

La figura 2 es un diagrama de bloques que ilustra la difusión en continuo protegida por DRM y protegida en integridad, a un cliente de contenido 214. Hay una entidad propietaria de contenido, que es, por ejemplo, un nodo propietario de contenido 210. Desde el nodo propietario de contenido 210, los contenidos se proporcionan a un número de servidores de difusión en continuo, tales como un servidor de difusión en continuo 212, que proporciona corrientes encriptadas a un número de clientes de contenidos, tales como el cliente de contenido 214. Los contenidos forman una presentación multimedia, que comprende típicamente dos componentes de medios, un componente de medio para el vídeo y un componente de medio para el audio. Los componentes de medios comprenden las grabaciones de vídeo y de audio en un formato codificado. El video puede ser codificado, por ejemplo, utilizando la codificación MPEG-4 del Grupo de Expertos de Películas (MPEG). El audio puede ser codificado, por ejemplo, utilizando la codificación de la Multi Relación Adaptada (AMR) de codificación utilizada en el sistema GSM para comunicaciones móviles. Los contenidos para una presentación de medio se difunden en continuo desde el servidor de difusión en continuo 212, por ejemplo, como por lo menos una corriente de Protocolo de Momento Real. El Protocolo de Momento Real (RTP) se especifica en la Petición de Comentarios (RFC) número 1889 del Grupo de Trabajo de Ingeniería de Internet (IETF). Una corriente de RTP se utiliza para transportar una corriente de medio, es decir, una corriente de contenidos que comprende, por ejemplo, datos codificados de vídeo o de audio. En una realización de la invención, hay una corriente de RTP para cada componente del medio asociado a una presentación multimedia, uno para audio y otro para vídeo. En una realización de la invención, los componentes de medio también pueden ser multiplexados en una única corriente de RTP.

El cliente de contenido 214 solicita de un servidor de difusión en continuo 212 el inicio de la corriente, por ejemplo, utilizando el Protocolo de Inicio de Sesión (SIP) especificado en el RFC 2543 o mediante el Protocolo de Difusión en Continuo en Tiempo Real (RTSP) especificado en el RFC 2326. Las propiedades de la corriente de contenidos de los componentes de medio asociados a una presentación multimedia se describen en el Protocolo de Descripción de Sesión (SDP) especificado en el IETF 2327. El SDP especifica un formato de documento de descripción para describir las corrientes de contenidos, sus propiedades y las direcciones de transporte asociadas. Una descripción SDP, en otras palabras brevemente expresadas como SDP, es proporcionada por un servidor de difusión en continuo como respuesta a una solicitud de información de difusión en continuo o como respuesta a una solicitud de iniciar la difusión en continuo. Con la descripción SDP, un cliente de contenido puede determinar, por ejemplo, las direcciones de corriente RTP y la codificación de los medios utilizados en las corrientes.

El cliente de contenido 214 es utilizado como un dispositivo de presentación de contenido, en el que el usuario puede ver y escuchar las presentaciones difundidas en continuo. Los derechos para ver una corriente de contenidos son obtenidos por el cliente de contenido 214 desde un nodo emisor de derechos 216. Los derechos comprenden al menos una Clave de Encriptado de Contenidos (CEK), que es utilizada

por el motor de DRM para desencriptar los contenidos de la difusión en continuo. Los derechos también pueden comprender la información asociada, por ejemplo, con el período de validez de los derechos. Debido al hecho de que la clave de encriptado de contenido es una clave simétrica, también se utiliza como clave de desencriptado de contenido. La clave de encriptado de contenido se proporciona al motor de DRM en un formato, en el que se ha encriptado mediante una clave asimétrica asociada con el motor de DRM para el cliente de contenido receptor. La clave asimétrica puede ser, por ejemplo, una clave pública para el motor de DRM en el cliente de contenido 214. De esta forma sólo el motor de DRM para el cliente de contenido 214 que tiene en su poder la clave privada puede obtener la clave de encriptado de contenido.

En primer lugar, en el momento t_1 el nodo propietario de contenido 210 genera una Clave de Encriptado / Desencriptado de Contenido (CEK), que es una clave simétrica, y una clave de integridad maestra (K). A continuación, el nodo propietario de contenido proporciona la K, utilizando la K encriptada la CEK, designada como E_{CEK} (K) en la figura 2, y la al menos una corriente encripta utilizando la CEK, designada como E_{CEK} (STREAM) en la figura 2, al servidor de difusión en continuo 212. La E_{CEK} (STREAM), la E_{CEK} (K) y K son entregados al servidor de corriente 212, por ejemplo, utilizando el Protocolo de Transferencia de Archivos (FTP), el Protocolo de Transferencia de Hipertexto (HTTP) o el HTTPS (HTTP Seguro) que se descarga como se muestra con la flecha 201. En lugar de descargar, también se podría utilizar para ellos la entrega basada en medios físicos. Pueden ser entregados como archivos separados o como un único archivo. Cuando el servidor de difusión en continuo 212 ha recibido al menos la K, en el momento t_2 genera un valor de inicialización aleatorio, designado como SEED en la figura 2, y calcula una clave de integridad de sesión (IK) mediante la fórmula IK = H (SEED, K), en la que K es la clave de integridad maestra, SEED es el valor de inicialización aleatorio y H () es una función hash unidireccional. El nodo propietario de contenido 210 proporciona la CEK al nodo emisor de derechos 216, como se ilustra con la flecha 202. Cuando el cliente de contenido 214 desea iniciar la difusión en continuo de la presentación multimedia, envía una solicitud de derecho, en la que se identifica a sí mismo, al nodo emisor de derechos 216, como se ilustra con la flecha 203. La identidad del cliente de contenido se designa como C en la figura 2. Como respuesta a la solicitud de derecho, el nodo emisor de derechos 216 responde con la CEK, que ha sido encriptada mediante una clave pública (C-PUB) del cliente de contenido 214, como se ilustra con la flecha 204. La CEK se desencripta en el motor de DRM en asociación con el cliente de contenido 214. La CEK sólo es conocida por el motor de DRM. Entonces, el cliente de contenido 214 puede empezar a recibir un corriente de contenidos que han sido encriptada utilizando la CEK, es decir, la E_{CEK} (STREAM) en la figura 2, desde el servidor de difusión en continuo 212.

El cliente de contenido 214 envía una solicitud de información de difusión en continuo, por ejemplo, una operación Describe RTSP, al servidor de difusión en continuo 212. El servidor de difusión en continuo 212 responde con un mensaje que comprende al menos los elementos de información H_{IK}(SDP), SEED y E_{CEK} (K), comprendidos en una descripción SDP. La H_{IK}(SDP) es un código hash calculado a partir de la descripción SDP devuelta por el servidor de difusión en continuo 212. La H_{IK}(SDP) es un código de autenticación de mensajes, que verifica que la descripción SDP no se ha visto obstaculizada en tránsito desde el servidor de difusión en continuo 212 al cliente de contenido 214. Cuando el cliente de contenido 214 ha recibido la E_{CEK} (K), envía la E_{CEK} (K) a su motor de DRM, que obtiene la K desencriptando la E_{CEK} (K) con la CEK. A continuación, en el momento t_3 el motor de DRM asociado con el cliente de contenido 214 también calcula IK = H (SEED, K) y obtiene la clave de integridad de sesión (IK), que es la misma que la calculada por el servidor de difusión en continuo 212 en el momento t_2. A continuación, el cliente de contenido 214 puede empezar a recibir una corriente encriptada utilizando la CEK desde el servidor de difusión en continuo 212. El inicio de la difusión en continuo puede ser solicitado por separado desde el servidor de difusión en continuo 212 o la corriente puede ser proporcionada continuamente a través de multidifusión o emisión sin solicitud separada del cliente de contenido 214. La corriente encriptada E_{CEK} (STREAM) se envía al motor de DRM asociado con el cliente de contenido 214. En el motor de DRM, la corriente E_{CEK} (STREAM) se desencripta con la CEK para obtener la corriente de contenidos de texto, que se designa en la figura 2 como STREAM.

En una realización de la invención, el servidor de difusión en continuo 212 prepara una descripción de SDP pregenerada, que se entrega al cliente de contenido 214. El servidor de difusión en continuo 212 puede decidir cambiar el valor de inicialización y responder a una orden de configuración RTSP emitida por el cliente de contenido 214 utilizando una orden de redireccionamiento RTSP. La recepción de orden de redireccionamiento RTSP en el cliente de contenido 214 resulta en que envía una orden Describe RTSP repetidamente para obtener al menos un nuevo valor de inicialización del servidor de difusión en continuo 212.

En una realización de la invención, la IK se aplica de manera que una secuencia de bytes de longitud predefinida se extrae tanto del servidor de difusión en continuo 212 como del cliente de contenido 214. La corriente de bytes puede ser, por ejemplo, un paquete, un conjunto de paquetes o cualquier trama de contenidos. A continuación, se calcula un código hash a partir de la corriente de bytes. El código hash se encripta utilizando la IK. El código hash encriptado es proporcionado por el servidor de difusión en continuo 212 en asociación con la corriente encriptada E_{CEK} (STREAM) al cliente de contenido 214, que proporciona el código hash encriptado junto con la corriente de encriptado al motor de DRM. El motor de

DRM desencripta el código hash con la IK y calcula de la misma forma un segundo código hash utilizando la misma secuencia de bytes. Si los códigos hash coinciden, la corriente de contenidos recibida E_{CEK} (STREAM) se considera que no ha sufrido alteraciones.

En una realización de la invención, se forma una clave de integridad de sesión separada para cada una de la al menos una corriente de contenidos en el nodo de difusión en continuo, es decir, un servidor de difusión en continuo. También se genera un valor de inicialización separado para cada una de la al menos una corriente de contenidos. Los valores de inicialización se proporcionan desde el nodo de difusión en continuo al dispositivo electrónico. Las claves de integridad de sesión se forman con los valores de inicialización y la clave de la integridad maestra en el dispositivo electrónico. Desde el nodo de difusión en continuo al dispositivo electrónico, se proporciona la al menos una corriente de contenidos y los datos de verificación de integridad asociados con cada una de la al menos una corriente de contenidos. La integridad de la al menos una corriente de contenidos está verificada en el dispositivo electrónico utilizando las claves de integridad de sesión, los datos de verificación de integridad asociados a cada una de la al menos una corriente de contenidos y la al menos una corriente de contenidos. En otras palabras, los valores de inicialización separados se utilizan en el dispositivo electrónico para formar claves de sesión asociadas a cada corriente de contenidos separada. Cada valor de inicialización se utiliza en el dispositivo electrónico para formar las mismas claves de integridad de sesión como se formaron en el nodo de difusión en continuo. A continuación, la integridad de una corriente de contenidos dada se verifica en el dispositivo electrónico utilizando la clave de integridad de sesión generada por esa corriente de contenidos particular, los datos de verificación de integridad asociados a esa corriente de contenidos en particular y la corriente de contenidos en sí. En una realización de la invención, distintas corrientes de contenidos utilizan la misma clave de integridad de sesión.

La figura 3 es un diagrama de flujo que muestra una realización de un procedimiento de protección de integridad para las corrientes protegidas por DRM en un cliente de contenido, tal como un cliente de contenido 214 en la figura 2. En el paso 300, el cliente de contenido obtiene una Clave de Encriptado de Contenido (CEK) de un nodo propietario de derechos. La obtención de la CEK se puede producir como respuesta a una transacción de pago para una presentación multimedia dada. En el paso 302, el cliente de contenido solicita una descripción de corriente asociada con una presentación multimedia solicitada desde un servidor de difusión en continuo. En el paso 304 el cliente de contenido obtiene como respuesta, al menos los elementos de información H_{IK}(SDP), SEED y E_{CEK} (K), comprendidos en una descripción SDP. La H_{IK}(SDP) es un código hash calculado a partir de la descripción SDP retornada por el servidor de difusión en continuo 212. La H_{IK}(SDP) es un código de autenticación de mensajes, que verifica que la descripción SDP no ha sido obstaculizada en el tránsito desde el servidor de difusión en continuo al cliente de contenido. En el paso 306, el cliente de contenido proporciona la SEED y E_{CEK} (K) a su motor de DRM. El motor de DRM descifra la K con la CEK y calcula una clave de integridad de sesión, que se referencia como IK en la figura 3, utilizando la fórmula IK = H (SEED, K), en la que IK es una clave de integridad maestra, SEED es el valor de inicialización aleatorio y H () es una función hash unidireccional. En el paso 308, el cliente de contenido recibe una corriente de contenidos encriptada E_{CEK} (STREAM) que también ha sido protegida utilizando la IK. La corriente de contenidos encriptada se transmite a través del motor de DRM a una aplicación de presentaciones multimedia en el cliente de contenido. El motor de DRM desencripta la corriente de contenidos utilizando la CEK. En el paso 310, el cliente de contenido verifica la integridad de la corriente de contenidos encriptada recibida E_{CEK} (STREAM) utilizando la IK. La verificación de integridad se puede basar, por ejemplo, en una secuencia de verificación recibida periódicamente que ha sido encriptada por el servidor de difusión en continuo con la IK. Si la integridad verificada es correcta, es decir, que no se ha detectado una violación de la integridad, el procedimiento continúa en el paso 308, en el que el cliente de contenido recibe más de la corriente de contenidos encriptada. Si la integridad no es correcta, en el paso 312 el cliente de contenido registra un error e interrumpe la presentación de la corriente de contenidos al usuario. Al usuario también se le proporciona un mensaje de error y un mensaje de informe de errores puede ser enviado al servidor de difusión en continuo.

En una realización de la invención, la obtención de la Clave de Encriptado de Contenido (CEK) de un nodo propietario de derechos es realizada por el cliente de contenido sólo como respuesta a la obtención de la descripción SDP. Por lo tanto, el paso 300 se realiza después del paso 304. La obtención de la CEK implica una transacción de pago para una presentación multimedia dada.

En una realización de la invención, el cliente de contenido verifica la integridad de la descripción SDP utilizando la IK después de que el cliente de contenido la haya calculado.

Se hace referencia a continuación a la figura 4, que es un diagrama de bloques que ilustra un terminal móvil 400 y un sistema para aplicar protección de integridad a corrientes protegidas por DRM en una realización de la invención. El terminal móvil (TM) 400 se encuentra en comunicación con una estación base 420, que está asociada a una red de acceso 410. A la red 410 está conectado al menos un servidor de difusión en continuo 416 y un servidor de derecho 418. El MT 400 comprende un motor de DRM 402, en otras palabras, un agente de DRM o una entidad de DRM, una aplicación de medio 404 y al menos un objeto de derecho. El MT 400 comprende también una entidad de comunicación 406, en otras

palabras, un medio de comunicación, que está configurado para recibir mensajes desde la red de acceso 410 y para realizar el tratamiento de capa del protocolo, por ejemplo, para los protocolos de capa física, capa de enlace y capa de red. En una realización de la invención, la entidad de comunicación 406 realiza el proceso de los paquetes IP y comprende la funcionalidad de procesamiento del Protocolo de Datagramas Universal (UDP) y del Protocolo de Verificación de Transmisión (TCP). La entidad de comunicación 406 está configurada para comunicarse con el motor de DRM 402 y la aplicación de medio 404. El MT 400 está configurado para enviar los mensajes recibidos en la entidad de comunicación 406 hacia adelante al motor de DRM 402 o a la aplicación de medio 404 sobre la base del contenido de los mensajes. En el MT 400 se puede almacenar al menos un objeto de medio, que se proporciona por medio del motor de DRM 402 a la aplicación de medio 404. El MT 400 también puede recibir una corriente encriptada que transporta un componente de medio. El MT 400 proporciona la corriente encriptada al motor de DRM 402, que desencripta la corriente utilizando una clave de desencriptado de contenidos revelada solamente al motor DRM 402. La corriente de contenidos encriptada se envía desde el servidor de difusión en continuo 416 al motor de DRM 402 a través del MT 400, como se ilustra en la figura 4 con la flecha 450. La flecha 450 también ilustra como se proporciona una descripción SDP que comprende elementos de información H_{IK}(SDP), SEED y E_{CEK} (K) al MT 400, antes de recibir la corriente de contenidos encriptada. Los elementos de información de descripción SDP están designados como I1 en la figura 4, mientras que la corriente de contenidos encriptada está designada como I2. El motor de DRM 402 desencripta un objeto de medio o una corriente de medios que se difunde en continuo al MT 400, si ha sido encriptada para protección. El encriptado se ha realizado en una fuente de contenidos utilizando un encriptado que sólo puede ser desencriptado utilizando una clave disponible al motor de DRM 402. El MT 400 almacena también al menos uno de los objetos de derechos 414 o recibe las corrientes de contenidos desde un servidor de difusión en continuo, tal como el servidor de difusión en continuo 416. El objeto de derecho 414 es utilizado por el motor de DRM 402 para verificar los derechos de usuario que se refieren a un objeto de medio dado tal como un objeto de medio almacenado en el MT 400. El motor de DRM 402 verifica los derechos de usuario antes de hacer disponible un objeto de medio a través de la aplicación de medio 404 para la presentación al usuario. El objeto de derecho 414 también puede comprender una clave de desencriptado de contenidos tal como la CEK divulgada asociada a las figuras 2 y 3. El objeto de derecho 414 se obtiene del servidor de derecho 418 en relación con un procedimiento de adquisición de derecho. El objeto de derecho 414 proporciona al menos la claves de encriptado / desencriptado de contenido CEK al motor de DRM 402, como se ilustra con la flecha 448 en la figura 4. La CEK está designada como el elemento de información I3 en la figura 4. Se debe hacer notar que, en una realización de la invención, un cliente de contenido es un terminal de red IP fija. En tal caso, el servidor de difusión en continuo y el servidor de derecho están conectados con el cliente de contenido utilizando una red de acceso fijo. Un terminal de red fija IP también comprende al menos un objeto de derecho, un motor de DRM y una aplicación de medio de una manera similar al MT 400.

Será evidente para un experto en la técnica que con el avance de la tecnología, la idea básica de la invención puede ser implementada de varias maneras. Por lo tanto, la invención y sus realizaciones no están limitadas a los ejemplos que se han descrito anteriormente; por el contrario, se pueden variar dentro del alcance de las reivindicaciones.

REIVINDICACIONES

1. Un procedimiento para recibir al menos una corriente de contenidos, que incluye:

requerir por medio de un dispositivo electrónico, información sobre la citada al menos una corriente de contenidos de un servidor de difusión en continuo;

recibir información en el citado dispositivo electrónico sobre la al menos una corriente de contenidos, la información que comprende al menos un valor de inicialización y una clave de integridad maestra encriptada con una clave de contenido;

desencriptar la citada clave de integridad maestra encriptada utilizando la citada clave de contenido en el citado dispositivo electrónico;

formar al menos una clave de integridad de sesión utilizando el citado al menos un valor de inicialización y la citada clave de integridad maestra en el citado dispositivo electrónico;

recibir del citado servidor de difusión en continuo en el citado dispositivo electrónico al menos una corriente de contenidos protegida en integridad, estando protegida la citada corriente de contenidos protegida en integridad con la citada al menos una clave de integridad de sesión;

verificar en el citado dispositivo electrónico la integridad de la citada al menos una corriente de contenidos protegida en integridad utilizando la citada al menos una clave de integridad de sesión, y desencriptar la citada al menos una corriente de contenidos protegida en integridad utilizando al menos en parte la clave de contenido.

2. El procedimiento de acuerdo con la reivindicación 1, en el que una verificación de integridad se realiza sobre el citado al menos un valor de inicialización y la citada clave de integridad maestra utilizando al menos una de la citada al menos una clave de integridad de sesión en el citado dispositivo electrónico.

3. El procedimiento de acuerdo con la reivindicación 1, en el que la formación de la citada al menos una clave de integridad de sesión y la citada verificación de integridad de la citada al menos una corriente de contenidos se lleva a cabo en el motor de Administración de Derechos Digitales (DRM) asociado al citado dispositivo electrónico.

4. El procedimiento de acuerdo con la reivindicación 1, comprendiendo el procedimiento adicionalmente:

enviar por el citado dispositivo electrónico una solicitud de derechos de contenido, identificando el citado dispositivo electrónico, a un nodo emisor de derecho;

recibir en el citado dispositivo electrónico desde un nodo emisor de contenidos, la citada clave de contenido en respuesta a la solicitud de derecho, en el que la clave de contenido se encripta utilizando una clave pública y el citado nodo emisor de contenido recibe la clave de contenido encriptada de un nodo propietario de contenido;

y

desencriptar la citada clave de contenido encriptada en el citado dispositivo electrónico.

5. El procedimiento de acuerdo con la reivindicación 1, comprendiendo el procedimiento adicionalmente:

proporcionar la citada clave de integridad maestra desde un nodo propietario de contenido al citado servidor de difusión en continuo, y

almacenar la citada clave de integridad maestra en el citado servidor de difusión en continuo.

6. El procedimiento de acuerdo con la reivindicación 1, en el que una corriente de paquetes IP comprende la citada al menos una corriente de contenidos.

7. El procedimiento de acuerdo con la reivindicación 1, en el que la clave de contenido comprende una clave simétrica.

8. El procedimiento de acuerdo con la reivindicación 1, en el que el dispositivo electrónico comprende una estación móvil.

9. Un procedimiento para proporcionar al menos una corriente de contenidos, que comprende:

recibir en un servidor de difusión en continuo una clave de integridad maestra, estando encriptada la clave de integridad maestra con una clave de contenido y al menos una corriente de contenidos encriptada, desde un propietario de contenido;

recibir una solicitud de información en al menos una corriente de contenidos desde un dispositivo electrónico;

generar por el citado servidor de difusión en continuo al menos un valor de inicialización;

enviar información al dispositivo electrónico por el citado servidor de difusión en continuo como respuesta a la solicitud de información en la al menos una corriente de contenidos, comprendiendo la información al menos un valor de inicialización y la clave de integridad maestra encriptada con una clave de contenido;

formar al menos una clave de integridad de sesión en el citado servidor de difusión en continuo utilizando el citado al menos un valor de inicialización y la citada clave de integridad maestra;

proteger en el citado servidor de difusión en continuo la integridad de al menos una corriente de contenidos utilizando la citada al menos una clave de integridad de sesión; y

transmitir la al menos una corriente de contenidos protegida en integridad utilizando al menos una clave de integridad de sesión al citado dispositivo electrónico.

10. El procedimiento de acuerdo con la reivindicación 9, en el que una corriente de paquetes IP comprende la citada al menos una corriente de contenidos.

11. El procedimiento de acuerdo con la reivindicación 9, en el que la clave de contenido comprende una clave simétrica.

12. Un dispositivo electrónico configurado para recibir al menos una corriente de contenidos, comprendiendo el dispositivo electrónico:

un motor de gestión de derechos digitales configurado para almacenar una clave de contenido, para desencriptar una clave de integridad maestra encriptada utilizando la citada clave de contenido, para formar al menos una clave de integridad de sesión utilizando al menos un valor de inicialización y la citada clave de integridad maestra, y verificar la integridad de la al menos una corriente de contenidos protegida en integridad utilizando la citada al menos una clave de integridad de sesión, y

una entidad de comunicación conectada en comunicación con el citado motor de gestión de derechos digitales, estando configurada la citada entidad de comunicación para enviar al menos una solicitud de información sobre la al menos una corriente de contenidos desde un servidor de difusión en continuo, para recibir información sobre al menos una corriente de contenidos, que comprende al menos un valor de inicialización y la citada clave de integridad maestra encriptada, y recibir desde el citado servidor de difusión en continuo la citada al menos una corriente de contenidos protegida en integridad.

13. El dispositivo electrónico de acuerdo con la reivindicación 12, en el que el motor de gestión de derechos digitales está configurado para realizar una verificación de integridad en el citado al menos un valor de inicialización y la citada clave de integridad maestra encriptada utilizando al menos una clave de integridad de sesión.

14. El dispositivo electrónico de acuerdo con la reivindicación 12, en el que la citada entidad de comunicación está configurada para recibir una clave de contenido encriptada y el citado motor de gestión digital de derechos está configurado para desencriptar la citada clave de contenido encriptada.

15. El dispositivo electrónico de acuerdo con la reivindicación 12, en el que una corriente de paquetes IP comprende la citada al menos una corriente de contenidos.

16. El dispositivo electrónico de acuerdo con la reivindicación 12, en el que la clave de contenido incluye una clave simétrica.

17. El dispositivo electrónico de acuerdo con la reivindicación 12, en el que el dispositivo electrónico comprende una estación móvil.

18. Un nodo de red que comprende una entidad de difusión en continuo configurada para recibir al menos una clave de integridad maestra, estando encriptada la clave de integridad maestra con una clave de contenido y al menos una corriente de contenidos encriptada, para recibir una solicitud de información sobre la al menos una corriente de contenidos, para generar al menos un valor de inicialización, para enviar información como respuesta a la solicitud de información sobre la al menos una corriente de contenidos, comprendiendo la información el citado al menos un valor de inicialización y la clave de integridad maestra encriptada con una clave de contenido, para formar al menos una clave de integridad de sesión utilizando el citado al menos un valor de inicialización y la citada clave de integridad maestra, para proteger la integridad de la citada al menos una corriente de contenidos utilizando la citada al menos una clave de integridad de sesión y transmitir la al menos una corriente de contenidos protegida en integridad utilizando la citada al menos una clave de integridad de sesión.

Un programa informático que comprende un código adaptado para realizar los pasos siguientes cuando se ejecuta en un sistema de procesamiento de datos:

solicitar una información del dispositivo electrónico sobre al menos una corriente de contenidos de un servidor de difusión en continuo;

recibir información en el citado dispositivo electrónico sobre la al menos una corriente de contenidos, comprendiendo la información al menos un valor de inicialización y una clave de integridad maestra encriptada con una clave de contenido;

desencriptar la citada clave de integridad maestra encriptada utilizando la citada clave de contenido en el citado dispositivo electrónico;

formar al menos una clave de integridad de sesión utilizando el citado al menos un valor de inicialización y la citada clave de integridad maestra en el citado dispositivo electrónico;

recibir del citado servidor de difusión en continuo en el citado dispositivo electrónico la citada al menos una corriente de contenidos protegida en integridad, estando protegida la citada corriente de contenidos protegida en integridad con la citada al menos una clave de integridad de sesión;

verificar en el citado dispositivo electrónico la integridad de la citada al menos una corriente de contenidos protegida en integridad utilizando al menos una clave de integridad de sesión, y

desencriptar la citada al menos una corriente de contenidos protegida en integridad utilizando al menos en parte la clave de contenido.

19. El producto de programa informático de acuerdo con la reivindicación 19, en el que el producto de programa informático se almacena en un soporte legible por ordenador.

20. El producto de programa informático de acuerdo con la reivindicación 20, en el que el medio legible por ordenador incluye una tarjeta de memoria extraíble.

21. El producto del programa informático de acuerdo con la reivindicación 20, en el que el citado medio legible por ordenador comprende un disco magnético u óptico.

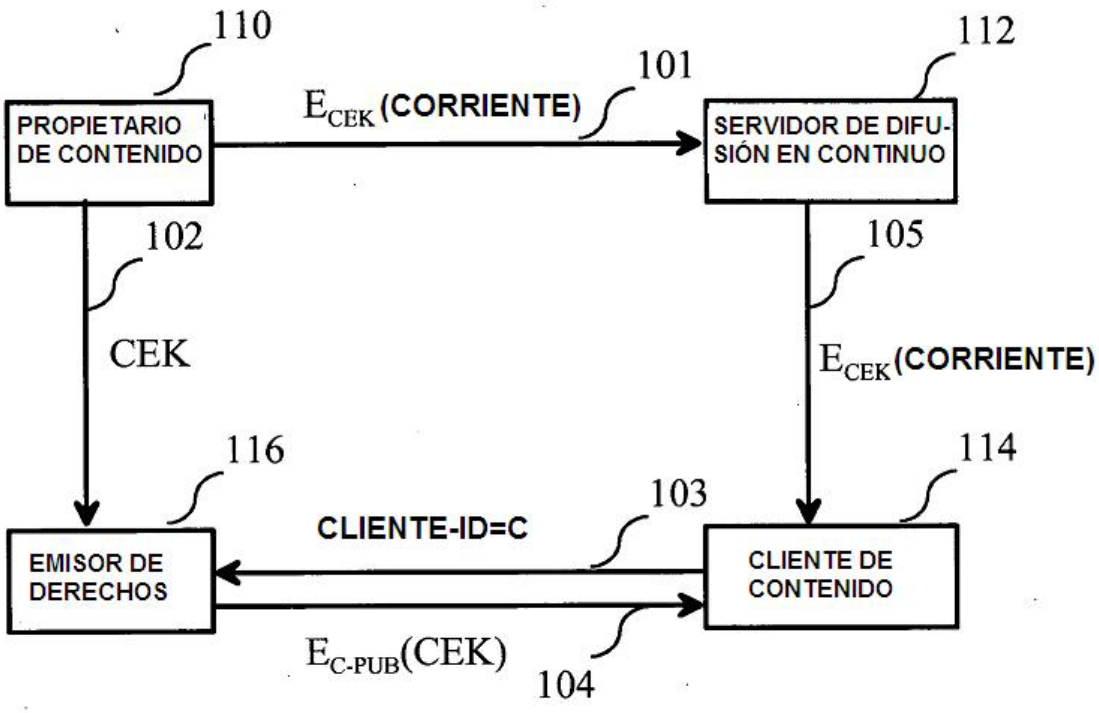

FIG. 1 (TÉCNICA ANTERIOR)

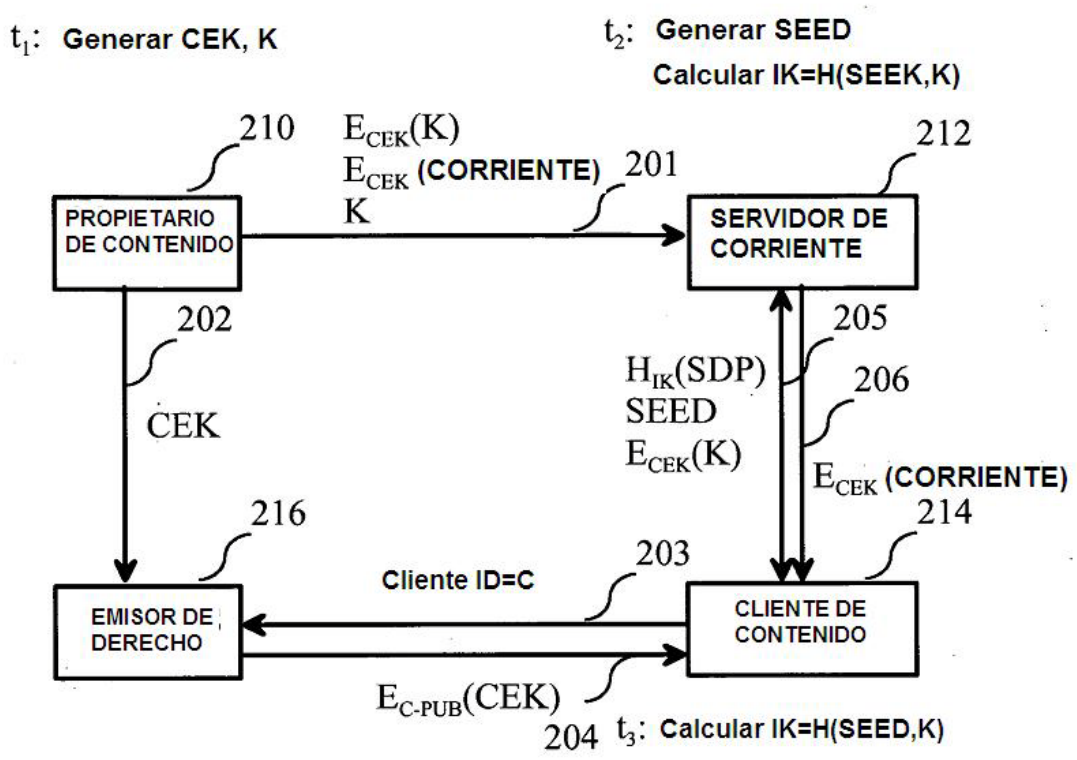
t1: Generar CEK, K
t2: Generar SEED
Calcular IK=H(SEEK,K)
210
E_CEK(K)
E_CEK (CORRIENTE)
K
201
212
PROPIETARIO DE CONTENIDO
SERVIDOR DE CORRIENTE
202
CEK
205
H_IK(SDP)
SEED
E_CEK(K)
206
E_CEK (CORRIENTE)
214
216
203
Cliente ID=C
EMISOR DE DERECHO
CLIENTE DE CONTENIDO
E_C-PUB(CEK)
204
t3: Calcular IK=H(SEED,K)

FIG. 2

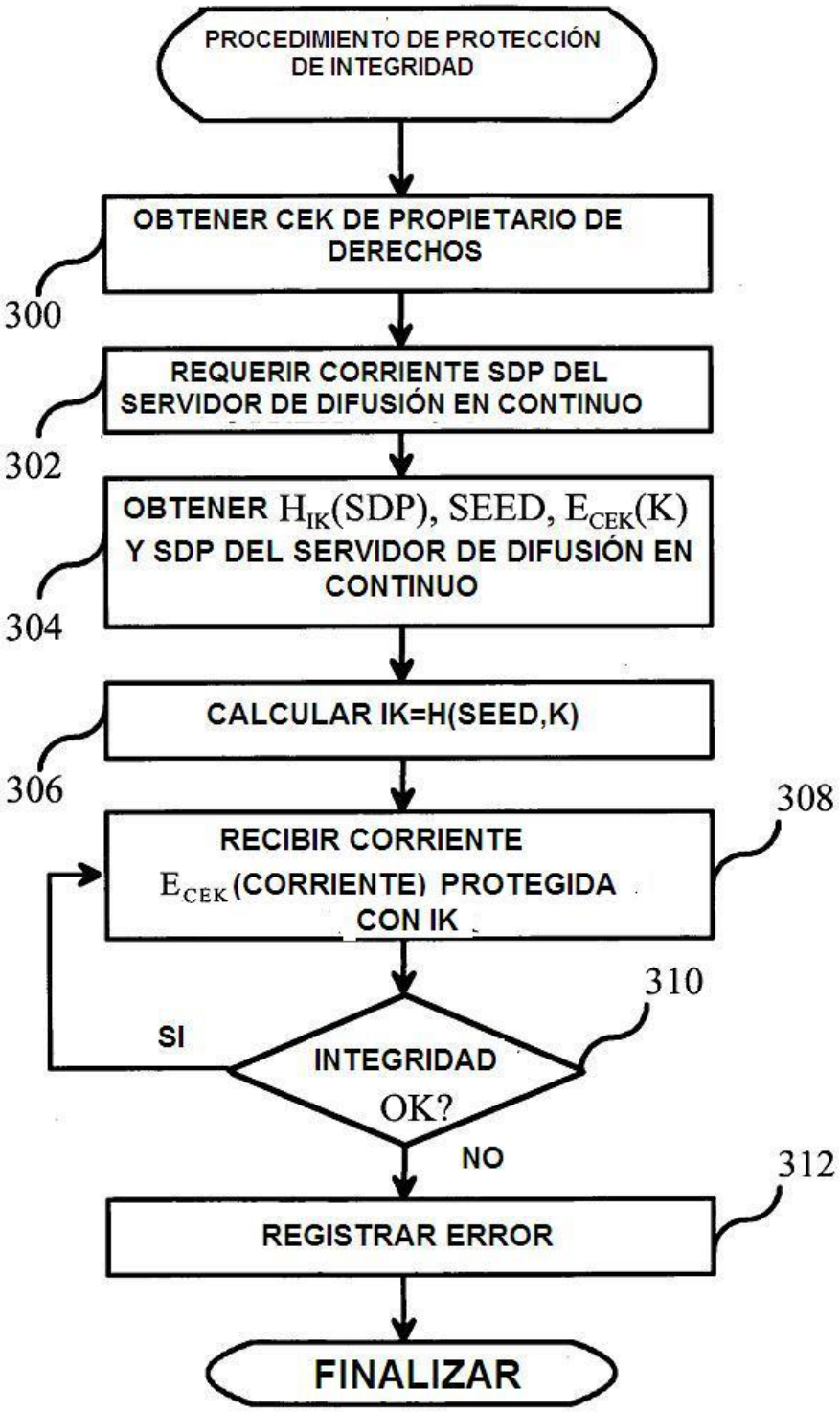
PROCEDIMIENTO DE PROTECCIÓN DE INTEGRIDAD
OBTENER CEK DE PROPIETARIO DE DERECHOS
300
REQUERIR CORRIENTE SDP DEL SERVIDOR DE DIFUSIÓN EN CONTINUO
302
OBTENER H_{IK}(SDP), SEED, E_{CEK}(K) Y SDP DEL SERVIDOR DE DIFUSIÓN EN CONTINUO
304
CALCULAR IK=H(SEED,K)
306
RECIBIR CORRIENTE E_{CEK}(CORRIENTE) PROTEGIDA CON IK
308
INTEGRIDAD OK?
310
SI
NO
REGISTRAR ERROR
312
FINALIZAR

FIG. 3

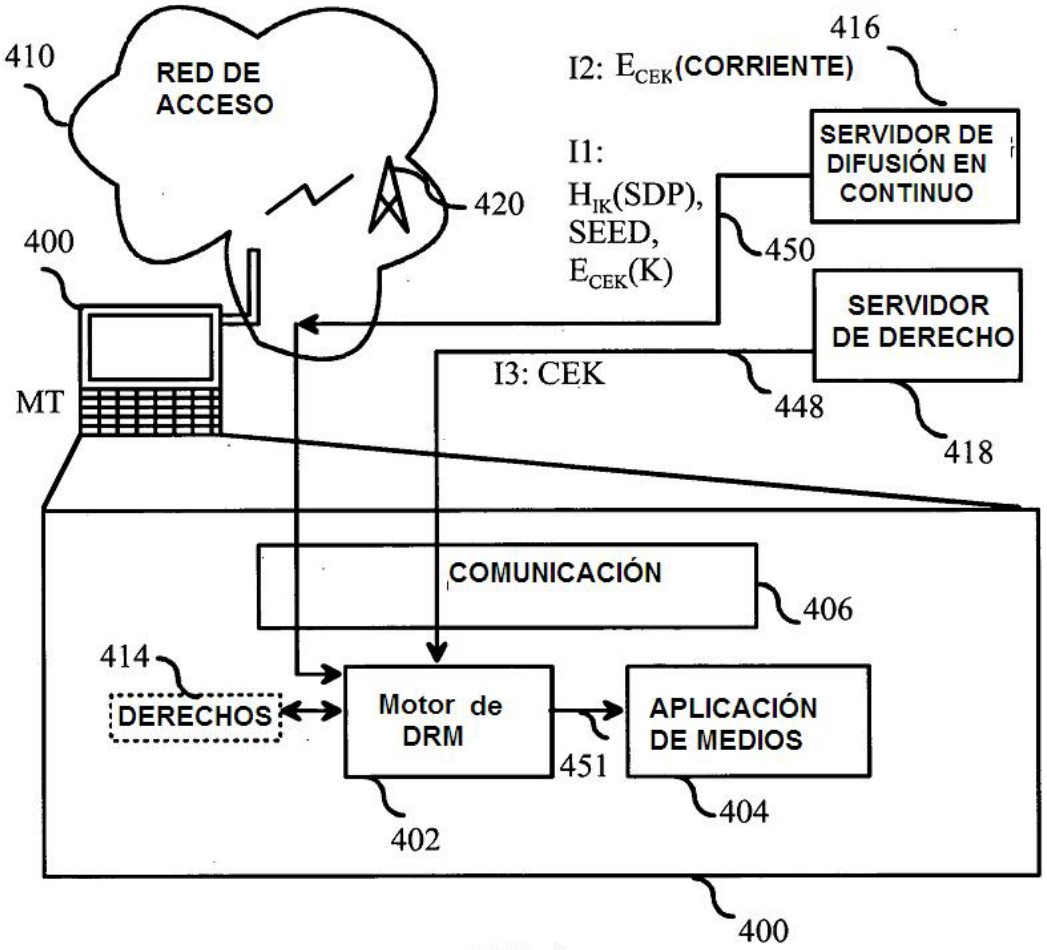
410
RED DE ACCESO
420
400
MT
416
I2: E_{CEK}(CORRIENTE)
SERVIDOR DE DIFUSIÓN EN CONTINUO
I1:
H_{IK}(SDP),
SEED,
E_{CEK}(K)
450
SERVIDOR DE DERECHO
I3: CEK
448
418
COMUNICACIÓN
406
414
DERECHOS
Motor de DRM
451
APLICACIÓN DE MEDIOS
404
402
400

FIG. 4