(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 657 798**

(51) Int. CI.:

H04L 29/06 (2006.01)
G06F 21/10 (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **20.02.2015 PCT/FR2015/050424**

(87) Fecha y número de publicación internacional: **11.09.2015 WO15132500**

(96) Fecha de presentación y número de la solicitud europea: **20.02.2015 E 15709296 (6)**

(97) Fecha y número de publicación de la concesión europea: **22.11.2017 EP 3114598**

(54) Título: **Método de suministro, a un terminal, de contenidos multimedia protegidos**

(30) Prioridad:

02.03.2014 FR 1451666

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
06.03.2018

(73) Titular/es:

VIACCESS (100.0%)
Les Collines de l'Arche, Tour Opéra C
92057 Paris La Défense Cedex, FR

(72) Inventor/es:

PHIRMIS, MATHIEU;
BOIVIN, MATHIEU;
CHIEZE, QUENTIN y
POCHON, NICOLAS

(74) Agente/Representante:

LEHMANN NOVO, María Isabel

DESCRIPCIÓN

Método de suministro, a un terminal, de contenidos multimedia protegidos

La invención se refiere a un método de suministro, a un terminal, de contenidos multimedia protegidos por un sistema de protección de contenidos multimedia. La invención se refiere, además, a un método de obtención, mediante un terminal, de contenidos multimedia protegidos para la puesta en práctica de este método para suministro de contenidos multimedia. Por último, la invención se refiere a un terminal y a un soporte de registro de informaciones para la puesta en práctica de este método de obtención de contenidos multimedia.

Los métodos dados a conocer pueden ponerse en práctica en concepto de cualquier servicio para suministro de contenidos multimedia protegidos, en cualquier sistema de suministro, en relación con contenidos multimedia protegidos, en donde una cabecera de red asegura la protección de los contenidos y su transmisión a una pluralidad de terminales.

Un cliente del servicio utiliza un terminal para acceder a un contenido con el fin de reproducirlo. El acceso a un contenido multimedia, en este documento, significa cargarlo en memoria y eliminar la protección, a medida mientras se está recibiendo, o en un soporte de registro en donde se ha registrado previamente, registrarlo o hacer cualquier otro uso ofrecido por el servicio de suministro de contenidos multimedia protegidos.

Los contenidos suministrados son:

- contenidos audiovisuales, a modo de ejemplo, programas de televisión,
- contenidos de audio solamente, por ejemplo, un programa radiofónico, o
- de manera más general, cualquier contenido digital que contenga vídeo y/o audio, tal como una aplicación informática, un juego, una presentación de diapositivas, una imagen o cualquier conjunto de datos.

Entre estos contenidos, se considerará más particularmente, a continuación, los así denominados contenidos temporales. Un contenido multimedia temporal es un contenido multimedia en donde la reproducción es una sucesión en el tiempo de sonidos, en el caso de un contenido temporal de audio, o de imágenes, en el caso de un contenido temporal de vídeo, o de sonidos e imágenes temporalmente sincronizados entre sí en el caso de un contenido multimedia temporal audiovisual. Un contenido multimedia temporal puede, además, incluir componentes temporales interactivos, temporalmente sincronizados con los sonidos o imágenes.

Para proporcionar dicho contenido, ha de codificarse en primer lugar, es decir, comprimirse, de modo que su transmisión requiera un menor ancho de banda.

Con esta finalidad, la componente de vídeo del contenido está codificada según un formato de vídeo, tal como, a modo de ejemplo, MPEG-2. El lector interesado podrá encontrar una presentación completa de este formato en el documento publicado por la Organización Internacional de Normalización bajo la referencia ISO/IEC 13818-2: 2013, titulado: "Tecnologías de la información - Codificación genérica de las imágenes en movimiento y del sonido asociado - Parte 2: Datos de vídeo". Hay muchos otros formatos, tales como MPEG-4 ASP, MPEG-4 Parte 2, MPEG-4 AVC (o Parte 10), HEVC (High Efficiency Video Coding) o WMV (Windows Media Video) pueden utilizarse alternativamente, y se basan en los mismos principios. Por lo tanto, todo lo indicado a continuación se aplica, además, a estos otros formatos de vídeo que se basan en el mismo principio que la codificación de MPEG-2.

La codificación MPEG-2 utiliza métodos generales de compresión de datos. Para las imágenes fijas, utiliza, en particular, la redundancia espacial interna de una imagen, la correlación entre los puntos próximos y la menor sensibilidad del ojo a los detalles. Para imágenes animadas, utiliza la fuerte redundancia temporal entre imágenes sucesivas. La utilización de lo que antecede hace posible codificar ciertas imágenes del contenido, aquí llamadas deducidas, con referencia a otras, aquí referidas como fuentes, a modo de ejemplo mediante predicción o interpolación, de modo que su decodificación solamente sea posible después de la de dichas imágenes fuentes. Otras imágenes, indicadas aquí como iniciales, se codifican sin referencia a dichas imágenes fuentes, es decir que cada una contiene, cuando están codificadas, el conjunto de informaciones necesarias para su decodificación y, por lo tanto, pueden decodificarse completamente con independencia de otras imágenes. Las imágenes iniciales son, por lo tanto, el punto de entrada obligatorio para acceder al contenido. Por lo tanto, el contenido codificado resultante no incluye los datos necesarios para decodificar cada una de las imágenes con independencia de las otras, sino que está constituido por "secuencias" según la terminología de MPEG-2. Una secuencia efectúa la compresión de al menos un "grupo de imágenes" (o GOP, por Group Of Pictures, en MPEG-2). Un grupo de imágenes es una serie de imágenes consecutivas en las que cada imagen es:

- inicial y origen para al menos una imagen deducida contenida en la misma secuencia de imágenes consecutivas,

- se deduce de tal modo que cada una de las imágenes fuentes necesarias para su descodificación pertenece a la misma secuencia de imágenes consecutivas.

Un grupo de imágenes no contiene una secuencia de imágenes consecutivas más pequeñas y que tienen las mismas propiedades, tal como se describió anteriormente. El grupo de imágenes es, por lo tanto, la parte más pequeña del contenido al que se puede acceder sin tener que decodificar primero otra parte de ese contenido.

Una secuencia está delimitada por una “cabecera” y un “extremo final”, estando cada uno identificado por un primer código específico. La cabecera tiene parámetros que caracterizan las propiedades previstas de las imágenes decodificadas, tales como las magnitudes horizontales y verticales, la relación y la frecuencia. La norma recomienda repetir la cabecera entre los grupos de imágenes de la secuencia, de modo que sus sucesivas presencias estén espaciadas, en el contenido codificado, en aproximadamente unos segundos.

A modo de ejemplo, un grupo de imágenes incluye, comúnmente, más de 5 a 10 imágenes y, en general, menos de 12 o 20 o 50 imágenes. Por ejemplo, en un sistema de 25 imágenes por segundo, un grupo de imágenes suele representar un tiempo de reproducción mayor que 0.1 o 0.4 segundos, y en general, menor que 0.5 o 1 o 10 segundos.

Un contenido multimedia temporal puede incluir varios componentes de vídeo. En este caso, cada uno de estos componentes se codifica tal como se describió con anterioridad.

La componente de audio del contenido se codifica también de conformidad con un formato de audio, tal como MPEG-2 Audio. El lector interesado puede encontrar una presentación completa de este formato en el documento publicado por la Organización Internacional para Normalización, bajo la referencia ISO/IEC 13818-3:1998, y con el título: “Tecnología de la Información – Codificación genérica de imágenes en movimiento e informaciones acústicas asociadas – Parte 3: Sonido”. Muchos otros formatos, tales como MPEG-1 Layer III, conocido mejor bajo la apelación MP3, AAC (Advanced Audio Coding), Vorbis o WMA (Windows Media Audio), pueden utilizarse, de forma alternativa, y están basados en los mismos principios que la codificación MPEG-2 Audio.

La codificación de MPEG-2 Audio obedece los mismos principios descritos anteriormente para un contenido temporal de vídeo. El contenido codificado resultante se define análogamente como “tramas”. Una trama es la análoga, en audio, de un grupo de imágenes en vídeo. La trama es, por lo tanto, la parte más pequeña del contenido de audio a la que puede accederse sin tener que decodificar otra parte de este contenido de audio. La trama incluye, además, el conjunto de las informaciones útiles para su decodificación.

Una trama suele tener más de 100 o 200 muestras, codificando cada una de ellas, un sonido y suele tener, en general, menos de 2000 o 5000 muestras. En condiciones normales, cuando se reproduce por un dispositivo multimedia, una trama dura más de 10 ms o 20 ms y, en general, menos de 80 ms o 100 ms. A modo de ejemplo, una trama incluye 384 o 1152 muestras, codificando cada una, un sonido. Dependiendo de la frecuencia de muestreo en la señal, esta trama representa un tiempo de reproducción de 8 a 12, o 24 a 36 milisegundos.

Un contenido multimedia temporal puede incluir varios componentes de audio. En este caso, cada uno de estos componentes está codificado tal como se describió con anterioridad.

Las componentes codificadas del contenido, también referidas como trenes elementales de datos, a continuación, se multiplexan, es decir, en particular, se sincronizan temporalmente y luego, se combinan en un solo tren, o flujo, de datos.

Dicho contenido, en particular cuando es el objeto de derechos tales como derechos de autor o derechos conexos, se proporciona protegido por un sistema de protección de contenido multimedia. Este sistema hace posible garantizar el respeto de condiciones de acceso al contenido que se derivan de estos derechos.

En general, se proporciona cifrado bajo su protección por un sistema de gestión de derechos digitales, o DRM por Gestión de Derechos Digitales, Digital Rights Management, en inglés. Este cifrado se suele realizar por medio de una clave de cifrado, mediante un algoritmo simétrico. Se aplica al flujo resultante de la multiplexación, o antes de la multiplexación, a los componentes del contenido codificado.

Un sistema DRM es, de hecho, un sistema para proteger los contenidos multimedia. La terminología del dominio de los sistemas de gestión de derechos digitales se utiliza más adelante en este documento. El lector interesado podrá, encontrar, por ejemplo, una presentación más completa en los siguientes documentos:

- Con respecto a la arquitectura general de un sistema DRM: DRM Architecture, Versión en borrador 2.0, OMA-DRM-ARCH-V2_0-20040518-D, Open Mobile Alliance, 18 de mayo de 2004,

- Más concretamente, para las licencias: Especificación DRM, versión borrador 2.1, OMA-TS-DRM-DRM-V2_1-20060523-D, Open Mobile Alliance, 23 de mayo de 2006.

En dicho sistema de gestión de derechos digitales, la obtención de una licencia permite a un terminal tener acceso al contenido multimedia protegido.

Una estructura bien conocida, tal como una licencia, incluye al menos un derecho de acceso a este terminal, para su acceso al contenido, y normalmente, un criterio temporal de validez. El derecho de acceso suele incluir una clave, denominada clave de contenido, necesaria para el descifrado del contenido multimedia protegido por un algoritmo de descifrado simétrico. El criterio temporal de validez caracteriza el período de tiempo en donde la licencia puede ser utilizada. Suele consistir, en condiciones normales, de uno o más intervalos de tiempo. Fuera de estos intervalos de tiempo, la licencia no permite el acceso al contenido.

La clave de contenido suele insertarse, generalmente, en la licencia en la forma de un criptograma, obtenido mediante cifrado de la clave de contenido con una clave de cifrado, denominada “de terminal”, específica para el terminal.

Para tener acceso al contenido, el terminal extrae de la licencia la clave de contenido, descifrando su criptograma, por medio de su clave de terminal.

El terminal descifra a continuación el contenido por medio de la clave de contenido así extraída de la licencia, con lo que se elimina la protección. A continuación, el terminal decodifica el contenido descifrado.

El terminal genera así un flujo multimedia ‘en limpio’ que comprende al menos una secuencia temporal de secuencias de vídeo o grupos de imágenes, o tramas de audio. Este flujo multimedia es capaz de reproducirse mediante un dispositivo multimedia conectado a dicho terminal. En este caso, por ‘en limpio’, se designa el hecho de que el flujo multimedia ya no necesita ser descifrado para ser reproducido por un dispositivo multimedia, en un modo directamente perceptible e inteligible por un ser humano. Por “dispositivo multimedia”, se designa, además, cualquier dispositivo capaz de reproducir el flujo multimedia ‘en limpio’, tal como, a modo de ejemplo, un televisor o un lector multimedia.

Con el fin de mejorar su protección, el contenido se proporciona por el sistema de entrega de contenido multimedia protegido, dividido en varios segmentos sucesivos de contenido protegido de forma individual, por medio del sistema de gestión de derechos digitales. Estos segmentos están ordenados, de forma temporal, los unos respecto a los otros.

Más concretamente, un segmento es una parte restringida del flujo multimedia ‘en limpio’ cuya reproducción tiene una duración menor de la reproducción del flujo multimedia por completo. Un segmento, por lo tanto, incluye una parte restringida de cada componente de vídeo y audio del flujo multimedia ‘en limpio’, cuya reproducción tiene una misma duración inferior a la de la reproducción del flujo multimedia completo. Estas partes restringidas de componentes están sincronizadas en el flujo para su reproducción, de forma simultánea. Por lo tanto, un segmento incluye la parte restringida de la secuencia temporal de secuencias de vídeo o grupos de imágenes, o tramas de audio que realizan la codificación de esta parte restringida de componente del flujo multimedia ‘en limpio’. Esta parte restringida está constituida por pluralidad de secuencias de vídeo o de grupos de imágenes, o de tramas de audio sucesivas. El término ‘sucesivas’ se entiende aquí como siguiéndose de inmediato, es decir, sin ninguna separación, en el desarrollo temporal del contenido, por otras secuencias de vídeo o grupos de imágenes, o tramas de audio que pertenecen a otro segmento. En condiciones normales, un segmento incluye más de diez, cien, mil o diez mil grupos de imágenes de vídeo sucesivas de una misma componente de vídeo codificado del flujo, o más de diez a cien veces de tramas de audio sucesivas de una misma componente de audio codificada del flujo.

Cada segmento se cifra mediante el algoritmo simétrico, como parte de su protección por el sistema de gestión de derechos digitales, mediante una clave de contenido específica. Esta clave de contenido se denomina "específica" puesto que solamente se utiliza para cifrar este segmento entre el conjunto de los segmentos del contenido multimedia. La obtención de una licencia específica, que incluya la clave de contenido específica necesaria para descifrar el segmento protegido, permite que un terminal acceda a este segmento.

Un segmento, por lo tanto, no se caracteriza por su estructura, sino por la clave de contenido específica utilizada para su cifrado. Un segmento es la pluralidad de secuencias de vídeo y tramas de audio, inmediatamente sucesivas, cifradas con una misma clave de contenido específico.

Con el fin de mejorar, además, la protección del contenido, se introduce un nivel intermedio de cifrado de las claves de contenido. Lo anterior permite cambiar, durante el curso del contenido, las claves de cifrado utilizadas para calcular los criptogramas de las claves de contenido específicas, que se incluyen en las licencias específicas.

Para esta finalidad, se reagrupan los segmentos en bloques de segmentos. Cada bloque contiene solamente una parte restringida de los segmentos de contenido. En condiciones normales, cada bloque contiene al menos un segmento y, generalmente, varios segmentos sucesivos. La expresión ‘sucesivo’ se entiende aquí como que se siguen de inmediato, es decir sin separaciones, en el desarrollo temporal del contenido, por segmentos que no

pertenecen al bloque considerado. Cada uno de estos bloques está asociado con una clave de cifrado de clave de contenido, denominada clave intermedia. La clave de contenido, necesaria para descifrar un segmento, se cifra con la clave intermedia asociada al bloque al que pertenece este segmento. El criptograma resultante se inserta, a continuación, en una licencia, denominada licencia intermedia, que se transmite conjuntamente con el segmento. La licencia intermedia incluye, además, un identificador de una licencia, denominado "de terminal". La licencia de terminal incluye un criptograma de la clave intermedia, obtenido mediante cifrado de esta clave intermedia con la clave de terminal.

Un bloque de segmentos, por lo tanto, no se caracteriza por su estructura, sino por la clave intermedia utilizada para cifrar la clave de contenido específica de cualquier segmento que le pertenece. En consecuencia, un bloque de segmento corresponde a los segmentos asociados con una licencia intermedia, en donde la clave de contenido específica es objeto de cifrado con una misma clave intermedia.

En tal sistema, un terminal recibe, por lo tanto, junto con un segmento cifrado, una licencia intermedia que incluye el criptograma de la clave de contenido específica, necesaria para descifrar el segmento. Este criptograma se obtuvo cifrando esta clave de contenido específica con una clave intermedia. Con el fin de acceder al segmento, el terminal debe obtener, en primer lugar, la licencia de terminal que incluye el criptograma de esta clave intermedia, obtenido cifrando esta clave con su clave de terminal. El terminal obtiene esta licencia de terminal por intermedio del identificador incluido en la licencia intermedia.

Con el fin de utilizar esta licencia de terminal, el terminal debe evaluar primero su criterio temporal con respecto a una fecha de servicio, controlado por el operador del servicio como una referencia temporal del servicio. Esta evaluación consiste en la determinación de si la fecha de servicio, generalmente expresada en segundos, está, o no, incluida en el período de validez de la licencia de terminal. El terminal debe conocer o conseguir, por lo tanto, la fecha de servicio.

Si el resultado de la evaluación del criterio temporal de la licencia de terminal es positivo, el terminal continúa utilizando la licencia de terminal, en particular, descifrado el criptograma de la clave intermedia que incluye, por medio de su clave de terminal. Si el resultado de esta evaluación es negativo, el terminal inhibe la utilización de la licencia de terminal y, en particular, no descifra el criptograma de la clave intermedia que contiene. Lo que antecede prohíbe la utilización de la licencia intermedia y el acceso al segmento protegido gracias a la clave de contenido que incluye el criptograma.

La fecha de servicio adquirida por el terminal condiciona, por lo tanto, su acceso al bloque de segmento al que pertenece el segmento recibido y, en consecuencia, el respeto de los derechos de los que este bloque es objeto. Ha de entenderse que es importante que la fecha de servicio no pueda modificarse fácilmente por un usuario del terminal. De hecho, podría establecerse entonces en una fecha incluida en el período de validez de la licencia de terminal, liberándose así de la fecha de servicio controlada por el operador, así como el respeto de los derechos cuyo segmento correspondiente es el objeto.

Para superar este inconveniente, ya se ha propuesto equipar los terminales con relojes locales de seguridad, es decir, relojes que no pueden ser ajustados por el usuario del terminal. Tales soluciones se describen, a modo de ejemplo, en las solicitudes US20090006854, US20060248596 y US2010024000A1.

La solicitud US2014/0033323 A1 da a conocer un método de actualización en un dispositivo móvil de un último tiempo adecuado conocido, en donde este último es objeto de avance y memorización cada vez que se produce un evento de iniciación.

Numerosos terminales todavía no tienen, sin embargo, un reloj de seguridad, es decir, con un mecanismo interno capaz de proporcionar localmente una fecha con una garantía que se considere suficiente para que esté lo suficientemente cerca de la fecha de servicio. La mayoría no tiene un reloj local, y los otros tienen uno no seguro, es decir, sin protección y, por lo tanto, el usuario puede modificarlo.

Con el fin de subsanar esta última dificultad, se ha propuesto integrar un servidor de fechas al sistema DRM. Un reloj local, en el interior del terminal, pero no protegido, que se sincroniza, además, de forma periódica con este servidor de fecha, a modo de ejemplo, de conformidad con el protocolo de hora de red, denominado NTP, por "Network Time Protocol", en inglés. Si el terminal no incluye un reloj local, o si no desea utilizar este reloj local, entonces, la fecha de servicio se adquiere a partir del servidor de fechas, de forma sistemática, cuando el criterio temporal de validez de una licencia deba ser evaluado.

Esta última forma de realización es ventajosa puesto que el uso del servidor de fechas es sistemático, se dispensa de utilizar un reloj local e impone la utilización de una fecha de servicio controlada por el operador. Sin embargo, lo que antecede tiene como resultado, normalmente, una carga significativa, y por lo tanto una carga de cálculo, del servidor de fechas, que requiere una gran cantidad de servidores para retener la carga. De hecho, cuando numerosos terminales requieren, en un corto intervalo de tiempo, el acceso a los contenidos ofrecidos por el servicio para proporcionar contenido multimedia protegido, es preciso, por lo tanto, evaluar el criterio temporal de validez de

las licencias correspondientes para cada uno de los terminales utilizados. Esto da como resultado una importante carga de cálculo para el servidor de fechas. Danto lugar, asimismo, a un tráfico de red importante hacia los servidores de fecha. Ahora bien, es probable que estas cargas de cálculo y el tráfico de red importantes sean susceptibles de perjudicar la calidad del servicio prestado.

Por lo tanto, es particularmente ventajoso reducir esta carga y este tráfico de red, al tiempo que se garantiza un alto nivel de seguridad del sistema frente a los intentos de manipular la fecha de servicio y sin que sea necesario usar un reloj local en el terminal.

La invención tiene como objeto alcanzar este objetivo.

La invención se refiere así a un método para proporcionar, a un terminal, contenidos multimedia protegidos de acuerdo con la reivindicación 1.

En dicho método, la asociación, en la etapa a), a cada uno de los segmentos, de su fecha de transmisión y la transmisión en el flujo, en la etapa b), de esta fecha junto con el segmento, permiten al terminal recibir, en la etapa c), esta fecha junto con el segmento y, por lo tanto, disponer de ella dentro de la fase de reproducción. Por lo tanto, el terminal está provisto con una nueva fuente de fecha, alternativa al servidor de fechas, y diferente de un reloj local, pero controlada por el operador del servicio que proporciona contenido multimedia protegido. Por lo tanto, proporciona fechas probablemente más cercanas a la fecha de servicio, y más difíciles de modificar que las de un reloj local. Estas fechas son por lo tanto más seguras.

En dicho método, la extracción del flujo, en la etapa g), junto con un segmento, de la fecha de transmisión del segmento, permite al terminal utilizar como fecha de servicio, esta fecha controlada por el operador de servicio, durante una realización de la etapa f), sin recurrir al servidor de fecha. La carga del servidor de fecha, así como el tráfico de red asociado, son así reducidos sin comprometer el nivel de seguridad del sistema.

La comparación, en la etapa g), de la fecha de transmisión extraída con la última fecha de servicio adquirida, permite restringir esta fecha de servicio para aumentar y así restringir tanto como sea posible el rango de posibles fechas de servicio entre dos solicitudes al servidor de fecha.

Por último, la transmisión en el flujo de la fecha de transmisión genera menos tráfico de red que la conexión a un servidor de fecha. De hecho, para cada fecha transmitida en el flujo no es necesario establecer y luego, terminar, una conexión con un servidor. Se utiliza, en este caso, una conexión ya establecida entre el terminal y una cabecera de red.

La invención se refiere, además, a un método para obtener, mediante un terminal, la puesta en práctica del método anterior, contenidos multimedia protegidos, de conformidad con la reivindicación 2.

Las formas de realización de este método para obtener contenidos multimedia protegidos pueden incluir una o más de las características de las reivindicaciones dependientes.

Estas formas de realización, de este método para obtener contenidos multimedia protegidos, presentan, además, las ventajas operativas siguientes:

- el mantenimiento sin cambios, en la etapa g), de la última fecha de servicio adquirida si la fecha de transmisión recuperada es anterior a esta fecha de servicio en no más de una primera duración predeterminada, permite la autorización de una reproducción diferida de un contenido que se está recibiendo;

- la comparación, en la etapa g), de la fecha de transmisión recuperada con la fecha de servicio adquirida durante la última realización de la etapa e), hace que sea posible obligar al terminal a adquirir la fecha de servicio a partir del servidor de fechas, cuando no se ha hecho, por lo menos, durante el segundo período predeterminado;

- la inhibición, en la etapa e), si no se puede establecer la conexión con el servidor de fechas, hace posible forzar la restricción de adquirir la fecha de servicio con el servidor de fechas;

- el conteo del número de veces consecutivas en las que no se puede establecer la conexión con el servidor de fechas, hace posible proteger la calidad del servicio prestado debido a la influencia de dificultades momentáneas de conexión con el servidor de fechas, mediante la autorización de la continuación del tratamiento del contenido multimedia incluso si no existe conexión con el servidor de fechas;

- la adquisición como una fecha de servicio, de cualquier fecha de transmisión recuperada después de la última fecha de servicio adquirida, hace posible forzar a la última fecha de servicio adquirida para su aumento en la misma tasa de cambio como en los segmentos recibidos.

La invención se refiere, además, a un soporte de registro de informaciones, incluyendo instrucciones para la puesta en práctica del método anterior de obtención de contenido multimedia, cuando dichas instrucciones se ejecutan por un ordenador.

La invención se refiere, por último, a un terminal para poner en práctica el método anterior estando, este terminal, de conformidad con la reivindicación 10.

La invención se entenderá mejor mediante la lectura de la descripción que sigue, dada únicamente a modo de ejemplo no limitativo, y con referencia a los dibujos en los que:

- la Figura 1 es una representación esquemática de la arquitectura de un sistema para suministro de contenidos multimedia protegidos,
- la Figura 2 es una representación esquemática de una licencia intermedia,
- la Figura 3 es una representación esquemática de una licencia de terminal,
- la Figura 4 es una representación esquemática de un flujo transmitido, por una cabecera de red, a un terminal dentro del sistema ilustrado en la Figura 1,
- la Figura 5 es una representación esquemática de un método para suministro de contenidos multimedia protegidos con la ayuda del sistema ilustrado en la Figura 1.

En estas figuras, las mismas referencias se proporcionan para designar los mismos elementos.

En el resto de esta descripción, las características bien conocidas por expertos en esta técnica no se describirán en detalle.

La Figura 1 ilustra un sistema para proporcionar contenido multimedia protegido. Este sistema comprende una pluralidad, normalmente de miles, de terminales conectados, por intermedio de una red 3, de una parte, a una cabecera 1 de red, y de otro parte, a un servidor de fechas 2. En este documento, se supone que la totalidad de dichos terminales son idénticos. De este modo, con el fin de simplificar la ilustración, solamente se muestra el terminal 4 en la Figura 1.

El terminal 4 puede acceder a un contenido para reproducirlo. Para este propósito, el terminal 4 comprende un ordenador 44 programable y una memoria 46. El ordenador 44 puede ejecutar instrucciones almacenadas en la memoria 46. La memoria 46 incluye las instrucciones necesarias para llevar a cabo el método de la Figura 5. La memoria 46 también incluye una última fecha de servicio adquirida TE y una fecha TT_s de servicio adquirida durante la última conexión con el servidor 2.

La red 3 es una red de distribución de información a gran distancia que permite establecer una comunicación bidireccional entre el terminal 4 y la cabecera de red 1 y el servidor 2. A modo de ejemplo, la red 3 es una red tipo telaraña mundial, más conocida en todo el mundo bajo la denominación de “red Internet".

La cabecera de red 1 es capaz de proteger un contenido y transmitirlo al terminal 4. Para este fin, la cabecera de red 1 comprende un reloj 12. Este reloj 12 proporciona a la cabecera de red 1 la fecha de transmisión de un segmento de contenido. Este reloj 12 está aquí sincronizado, de acuerdo con el protocolo de tiempo de red NTP (Network Time Protocol), con un primer reloj de referencia externo a la cabecera de red 1.

El servidor 2 de fechas puede proporcionar al terminal 4 una fecha de servicio en respuesta a una demanda. El servidor 2 está aquí sincronizado, de conformidad con el protocolo NTP, con un segundo reloj de referencia externo al sistema.

Los primero y segundo relojes de referencia son, o no, el mismo reloj. En virtud de la arquitectura jerárquica, en niveles denominados estratos, asociada con el protocolo NTP, los primero y segundo relojes de referencia son ellos mismos de la misma forma, cada uno sincronizado con un reloj de referencia del estrato inmediatamente superior, y así sucesivamente, de paso en paso y, en última instancia, cada uno sincronizado con un reloj de referencia del estrato 1. En cada estrato, estos relojes de referencia son, o no, el mismo reloj.

En este documento, para la cabecera de red 1 y el servidor 2, solo se describen en detalle las diferencias con respecto a una cabecera de red convencional y a un servidor de fecha convencional. Para información sobre una cabecera de red convencional y un servidor de fecha convencional, el lector puede referirse al estado de la técnica citado en la introducción de esta solicitud de patente.

La Figura 2 ilustra una licencia intermedia L_i. Esta licencia L_i incluye, en particular, un criptograma $(K_{si})*K_{Gp}$ 51 obtenido mediante el cifrado de una clave K_{si} con una clave intermedia K_{Gp}. La clave K_{si} es la clave utilizada para

cifrar el segmento S_i del contenido multimedia. La clave intermedia K_{Gp} es la clave utilizada para cifrar las claves K_{si} de todos los segmentos del bloque Gp. La licencia intermedia L_i también incluye:

- un identificador Id (K_{Gp}) 50 de esta clave intermedia K_{Gp}, y

- una fecha TS_i 53 de transmisión del segmento S_i.

Las referencias utilizadas en esta figura y en la Figura 3 se describen con más detalle con referencia a la Figura 5.

La Figura 3 ilustra una licencia de L_p, o licencia de terminal, de un sistema de gestión de derechos digitales. Esta licencia incluye un derecho de acceso 52 y un criterio temporal 54 de validez, tal como se define en la parte introductoria de esta solicitud de patente. El derecho de acceso 52, en este caso, comprende un criptograma de esta clave intermedia K_{Gp}. La licencia L_p también incluye el identificador Id (K_{Gp}) 50 de la clave intermedia.

La Figura 4 ilustra un flujo 6 transmitido por la cabecera de red 1 al terminal 4 durante la puesta en práctica del método de la Figura 5. El flujo 6 incluye varios bloques de segmentos de contenido multimedia. A modo de ejemplo, el flujo 6 tiene más de dos, diez o cien bloques de segmentos. Para simplificar la Figura 3, solo se han representado dos bloques 62, 63. En esta figura, el símbolo "..." entre los bloques 62, 63 indica que no se han representado bloques. En este caso, se supone que todos estos bloques son estructuralmente idénticos y difieren entre sí solo en el contenido codificado en cada uno de los segmentos. En particular, todos los bloques tienen el mismo número de segmentos. Por lo tanto, solo la estructura del bloque 62 se describirá ahora con más detalle.

El bloque 62 comprende una pluralidad de segmentos. En condiciones normales, el bloque 62 tiene más de diez o cien segmentos sucesivos. El bloque 62 tiene solo una parte restringida del conjunto de los segmentos cuya concatenación forma la totalidad del contenido. Aquí, solo se han representado tres segmentos 622, 623 y 624 en la Figura 4. El símbolo "..." entre los segmentos 623 y 624 indica que no se han representado otros segmentos. En este caso, todos estos segmentos son estructuralmente idénticos y difieren entre sí solo por las informaciones codificadas en cada uno de ellos. Por lo tanto, solo el segmento 622 se describe ahora con más detalle.

El segmento 622 cumple con la definición del término "segmento" dada en la introducción a este texto. Al segmento 622 está asociada una licencia intermedia 642, que se transmite junto a este segmento en el flujo 6. En este caso, esta asociación se realiza mediante sincronización del segmento 622 y de la licencia intermedia 642 dentro del flujo. En condiciones normales, esta sincronización se consigue mediante la adyacencia del segmento 622 y la licencia intermedia 642 en el flujo, y cuando llega el momento, por su transmisión conjunta.

El funcionamiento del sistema de la Figura 1 se describirá ahora con referencia al método de la Figura 5.

Inicialmente, durante una etapa 1000, de una manera conocida por los expertos en la técnica, la cabecera de red 1 obtiene un contenido multimedia temporal ‘en limpio’. A continuación, codifica este contenido.

A continuación, durante una etapa 1002, la cabecera de red 1 divide el contenido multimedia codificado en varios segmentos S_i sucesivos de contenido. Estos segmentos S_i están ordenados temporalmente entre sí, y su secuencia completa constituye el contenido. En el resto de esta descripción, el índice "i" es el número de orden del segmento S_i en esta serie temporal de segmentos.

La cabecera de red 1 asegura, a continuación, la protección individual, mediante un sistema de gestión de derechos digitales, de cada uno de los segmentos de S_i. A este efecto, durante una etapa 1004, se efectúa el cifrado de cada segmento S_i con una clave K_{si} de contenido específico, que no se puede utilizar para cifrar otro segmento de la misma secuencia de segmentos.

A continuación, durante una etapa 1006, la cabecera de red 1 constituye bloques G_p de segmentos sucesivos. El índice "p" es el número de orden del bloque en la serie de bloques sucesivos así constituidos. En este documento, la cabecera de red 1, fija, a este fin, el número de segmentos contenidos en cada bloque. Para cada bloque que comprende este número de segmentos sucesivos, genera una clave intermedia K_{Gp}. La clave intermedia K_{Gp} es diferente para cada bloque del contenido multimedia protegido. Luego se cifra la clave de cifrado K_{si} de cada uno de los segmentos S_i del bloque G_p con la clave intermedia K_{Gp}. Por lo tanto, obtiene para cada segmento S_i del bloque G_p el criptograma $(K_{si})*K_{Gp}$ 51. La cabecera de red 1, inserta, a continuación, el identificador id (K_{Gp}) 50 de la clave intermedia K_{Gp} y el criptograma $(Ksi)*K_{Gp}$ 51 en la licencia intermedia L_i que asocia a este segmento S_i, tal como se describe con referencia a la Figura 3.

En paralelo, a modo de ejemplo de una de las etapas 1000, 1002, 1004 y 1006, durante la etapa 1100, la cabecera de red 1 recibe, del terminal 4, una solicitud para obtener el contenido. Esta solicitud contiene, en particular, un identificador de una clave K_T del terminal. La clave K_T es única para cada terminal. De una manera conocida por los expertos en la técnica, la clave K_T fue obtenida por el terminal durante su fase de fabricación o personalización. La clave K_T se obtiene a continuación por la cabecera de red 1 en el momento de una fase de registro del terminal 4 antes de la puesta en práctica del método de la Figura 5.

En respuesta a la demanda recibida en la etapa 1100, la cabecera de red 1 pone en práctica las etapas 1200, 1202, 1204 y 1206.

En la etapa 1200, la cabecera de red 1, cifra cada clave intermedia K_{Gp}, utilizada con la clave K_T, del terminal 4 para obtener el criptograma $(K_{Gp})*K_T$. Luego, para cada bloque G_p, se inserta como derecho de acceso 52 a ese bloque, el criptograma $(K_{Gp})*K_T$ en la licencia L_p de terminal destinada al terminal 4. El identificador $Id(K_{Gp})$ 50 de la llave K_{Gp} intermedia también se inserta en la licencia L_p y en cada licencia L_i intermedia, asociada con cualquier segmento S_i del bloque G_p. La licencia L_p se asocia, de este modo, con cada uno de los segmentos S_i, y por lo tanto con el bloque G_p, por este identificador $Id(K_{Gp})$. Por último, la cabecera de red 1 inserta, en la licencia L_p, el criterio temporal 54 de validez de esta licencia. A modo de ejemplo, este criterio 54 especifica que la licencia de L_p solamente se puede utilizar entre el 1 de enero de 2014 y el 1 de marzo de 2014.

A continuación, durante una etapa 1202, la cabecera de red 1 asocia a cada uno de los segmentos S_i con su fecha de transmisión TS_i. En este caso, se obtiene la fecha de transmisión del segmento S_i con el reloj 12. Después, se inserta esta fecha TS_i de transmisión en la licencia L_i intermedia, asociada con el segmento S_i. Por lo general, esta fecha de transmisión es la del final del cálculo de la licencia L_i intermedia, asociada con el segmento S_i. Por lo tanto, precede, normalmente, en una fracción de segundo, al comienzo de la transmisión en la red 3 de este segmento S_i. Se inserta preferiblemente, protegida en su integridad, en la licencia de L_i.

La cabecera de red 1 genera, de este modo, etapa a etapa, el flujo 6 que comprende cada uno de los segmentos S_i del bloque G_p considerado y su licencia L_i intermedia asociada, que incluye, a su vez, la fecha de transmisión TS_i.

La cabecera de red 1 transmite, por último, en el terminal 4, durante la etapa 1204, la licencia L_p, y en la etapa 1206, el flujo 6.

De una manera conocida por los expertos en la técnica, de conformidad, en particular, con la naturaleza del servicio de suministro de contenido considerado y la solicitud del terminal, las etapas 1204 y 1206 pueden estar sincronizadas o ser independientes en el tiempo. A modo de ejemplo, en este caso, el servicio de suministro de contenido considerado, es un servicio de difusión de contenido, y la demanda recibida en la etapa 1100, tiene como objetivo obtener el contenido para reproducirlo a medida de su recepción. La etapa 1204 precede entonces a la etapa 1206 de difusión del contenido, de modo que la licencia L_p sea recibida y procesada por el terminal antes de que se reproduzca el bloque G_p. Lo mismo sucede si la demanda recibida en la etapa 1100 tiene como fin obtener el contenido para realizar, a medida que se recibe, cualquier otro uso controlado por el sistema de protección de contenido, tal como su registro.

En consecuencia, el terminal recibe, durante una etapa 1300, la licencia L_p, y en una etapa 1302 el flujo 6.

En correspondencia con las etapas 1204 y 1206, las etapas 1300 y 1302 pueden sincronizarse o ser independientes en el tiempo. A modo de ejemplo, en este caso, la etapa 1300 precede a la etapa 1302, de modo que la licencia L_p sea procesada por el terminal antes de que se reproduzca el bloque G_p.

A continuación, el terminal realiza una fase de reproducción del contenido. Durante esta fase, continúa sucesivamente para cada uno de los segmentos S_i del flujo 6 recibido en las etapas 1400 a 1422.

En la etapa 1400, el terminal extrae el segmento S_i y su licencia L_i, intermedia asociada, del flujo 6.

A continuación, durante la etapa 1402, el terminal extrae de la licencia L_i la fecha TS_i de transmisión del segmento S_i.

A continuación, durante la etapa 1404, el terminal compara la fecha de transmisión de TS_i con la última fecha de servicio adquirida, aquí denominada TE.

Si TS_i es posterior a TE, entonces, durante la etapa 1406, el terminal 4 sustituye el valor de la fecha TE por el valor de la fecha TS_i extraída en la etapa 1402. Luego, siempre durante la etapa 1406, el terminal 4 compara esta nueva fecha TE con la última fecha de servicio adquirida del servidor 2 de fechas, en este documento denominado TT_s.

Si TE es posterior a TT_s en al menos una duración predeterminada, aquí indicada como ETTD, entonces el terminal pasa a la etapa 1408 de adquisición de la fecha de servicio desde el servidor 2 de fechas. En caso contrario, el terminal avanza directamente a la etapa 1410. Lo que antecede fuerza al terminal 4 a conectarse regularmente al servidor 2.

La duración predeterminada ETTD podría inicializarse en el terminal 4 durante la producción del sistema, o por el operador del servicio. Su valor suele ser mayor a diez o veinte minutos. El valor de la duración ETTD también suele ser inferior a diez, cincuenta o cien horas.

Los valores de las fechas TE y TT_s, inicialmente podrían ser adquiridos por el terminal 4, durante una fase, por ejemplo, denominada de instalación, de activación o de personalización, con el servidor de fechas 2, o inicializadas, a modo de ejemplo, a cero.

En la etapa 1404, si TS_i es anterior a TE en más de una duración predeterminada, aquí indicado como TSW, entonces el terminal pasa directamente a la etapa 1408 de adquisición de la fecha de servicio desde el servidor de fechas 2. Por lo tanto, cuando no se puede confiar en la fecha de transmisión, es esencial utilizar la fecha de servicio comunicada por el servidor de fechas 2 que se utiliza.

Por último, en la etapa 1404, si TS_i está comprendido entre TE y TE-TSW, entonces el método continúa directamente en la etapa 1410. En este caso, la fecha TE no se actualiza en función de la fecha TS_i extraída durante la etapa 1402. Esta situación se produce cuando un segmento es reproducido por el terminal con un ligero retraso en comparación con el momento de recepción de este segmento por este terminal. El valor del pequeño retraso admisible, en este documento, es igual a TSW.

La duración predeterminada TSW podría inicializarse en el terminal 4 durante la producción del sistema, o por el operador del servicio. Su valor suele ser mayor a diez o veinte minutos. En general, su valor es, igualmente, inferior a una hora o diez horas.

En la etapa 1408, el terminal 4 efectúa la autenticación del servidor 2, a modo de ejemplo usando un certificado electrónico. El terminal 4 también transmite, al servidor de fecha 2, una solicitud de fecha y obtiene en respuesta una fecha. Solamente si el servidor 2 es objeto de autenticación satisfactoria, entonces el terminal 4 adquiere esta fecha y reemplaza el valor de la fecha TT_s y de la fecha TE, por el valor de esta fecha obtenida del servidor 2.

En este caso, en la etapa 1408, si la conexión con el servidor 2 de fechas, no puede establecerse, o si la autenticación se agota, el terminal 4 incrementa un contador de fallos de conexión. Si el valor de este contador no excede un umbral predeterminado, indicado como Max_tts_bypass, el terminal 4 pasa a la etapa 1410 sin cambiar los valores de las fechas TT_s y TE. Si el valor de este contador pasa el umbral Max_tts_bypass, el terminal 4 inhibe las etapas 1410 y siguientes del método, en particular, la extracción del derecho de acceso de la licencia L_p de terminal, lo que prohíbe el acceso al segmento S_i. A continuación, el valor del contador puede reinicializarse a su valor inicial por el operador del servicio. También se puede restablecer automáticamente después de un tiempo predeterminado, a modo de ejemplo, más de 30 minutos o 1 hora o 10 horas.

El umbral Max_tts_bypass podría inicializarse en el terminal 4 durante la producción del sistema, o por el operador del servicio. Su valor suele ser mayor que dos, tres o cinco y, a modo de ejemplo, menor de diez, veinte o cincuenta.

En la etapa 1410, el terminal 4 extrae de la licencia intermedia L_i el identificador $Id(K_{Gp})$ 50 de la clave intermedia K_{Gp}.

Luego, durante la etapa 1412, el terminal 4 busca, entre las licencias de terminal recibidas, la licencia de L_p que incluye el identificador $Id(KG_p)$ 50.

En la etapa 1414, el terminal 4 extrae el criterio temporal 54 de la licencia L_p encontrada en la etapa 1412. Luego evalúa este criterio con respecto a la última fecha TE de servicio adquirida. Si esta fecha de servicio satisface el criterio temporal 54, entonces, el terminal 4 pone en práctica las etapas 1416 y siguientes del método. Si no es así, inhibe las etapas 1416 y siguientes del método, en particular la extracción del derecho de acceso de la licencia L_p, lo que impide el acceso a los segmentos y vuelve a la etapa 1400 para tratar el siguiente segmento S_{i+1}.

En la etapa 1416, si la clave intermedia K_{Gp} contenida en el derecho de acceso 52 no se ha extraído ya desde el comienzo de la fase de reproducción, entonces el terminal 4 extrae de la licencia L_p, encontrada en la etapa 1412, el criptograma $(K_{gp})*K_T$.

A continuación, en la etapa 1418, el terminal 4 descifra el criptograma $(K_{Gp})*K_T$ con su clave K_T de terminal, obteniendo, de este modo, la clave K_{Gp} intermedia.

Luego, durante la etapa 1420, el terminal 4 descifra el criptograma $(K_{si})*K_{Gp}$ con la clave K_{Gp} intermedia, descifrada durante la etapa 1418, obteniendo así la clave específica K_{si}.

Por último, en la etapa 1422, el terminal 4 descifra el criptograma del segmento S_i con la clave específica K_{si}, obtenida durante la etapa 1420, con el fin de obtener el segmento S_i 'en limpio'. El segmento S_i 'en limpio' puede transmitirse, entonces, por el terminal 4 a cualquier dispositivo multimedia para ser reproducido. El método vuelve a la etapa 1400 para recibir y reproducir el siguiente segmento S_{i+1}.

Son posibles numerosas otras formas de realización de la invención. A modo de ejemplo, el contenido es proporcionado por el sistema para suministrar contenidos multimedia protegidos, cifrados con varias claves para su protección por el sistema de gestión de derechos digitales. Varias licencias, que contienen al menos una de estas

claves de contenido, son necesarias para que el terminal acceda al contenido. El proceso aquí reivindicado se aplica ahora a una, al menos, de estas licencias.

En otra forma de realización, el derecho de acceso 52 de la licencia L_p incluye la clave intermedia K_{Gp} y no el criptograma $(K_{Gp})*K_T$. En esta forma de realización, la licencia del terminal no es necesaria.

En la forma de realización anterior, el derecho de acceso es un criptograma de la clave K_{Gp} obtenida mediante el cifrado con la clave criptográfica K_T. Un criptograma es una información insuficiente para encontrar, por sí sola, la clave de contenido K_{si}. Por lo tanto, si se intercepta la transmisión de la licencia, el conocimiento del criptograma no permite encontrar la clave de contenido para descifrar un segmento del contenido multimedia. Para encontrar la clave de contenido 'en limpio', es decir, la clave de contenido para descifrar directamente el segmento del contenido multimedia, el criptograma debe combinarse con información secreta. En el ejemplo anterior, la información secreta es la clave criptográfica K_T, que permite descifrar el criptograma $(K_{Gp})*K_T$. Son posibles otras formas operativas de obtención del criptograma contenido en el derecho de acceso. A modo de ejemplo, el criptograma puede ser un puntero hacia una clave criptográfica almacenada 'en limpio' en una tabla que contiene una multitud de claves intermedias posibles. En este caso, la información secreta es la tabla que asocia con cada puntero una clave criptográfica 'en limpio'. El criptograma también puede ser:

- un identificador de esta clave criptográfica, que se proporcionará a la cabecera de red, a través de una ruta de retorno, lo que permite solicitar la clave desde la cabecera de red, y luego recibir, en respuesta y solamente después de una autenticación satisfactoria del terminal, la clave criptográfica o un valor de inicialización que permite al terminal reconstruir esta clave criptográfica;

- un enlace, normalmente, un URL (Localizador Uniforme de Recursos), que permite la lectura, normalmente solo en el caso de una autenticación satisfactoria del terminal, de esta clave criptográfica en un servidor de claves criptográficas; o

- un valor de inicialización, que permite al terminal reconstruir esta clave criptográfica, normalmente realizando un cálculo del valor de esta clave usando, a modo de ejemplo, un algoritmo secreto conocido solo por el terminal y la cabecera de red.

Como alternativa, el contenido se proporciona protegido por un sistema de gestión de derechos digitales sin cifrar. La clave de contenido no está incluida en los datos de acceso insertados en la licencia.

En otra forma de realización, el contenido multimedia se proporciona protegido por un sistema de acceso condicional, o CAS, por el Conditional Access System. A continuación, se utiliza la terminología del dominio de los sistemas de acceso condicional. El lector interesado puede, por ejemplo, encontrar una presentación más completa en el documento: "Modelo funcional de un Sistema de Acceso Condicional", Revisión de la EBU, Unión Técnica Europea de Radiodifusión, Bruselas, BE, Nº 266, 21 de diciembre de 1995. Un segmento es entonces un criptoperiodo, una licencia de terminal, un EMM, y la licencia intermedia un ECM. La fecha de transmisión normalmente se inserta en un ECM.

En otra forma de realización, el contenido se proporciona, por el sistema, protegido por cualquier otro tipo de sistema de protección de contenido, tal como, por ejemplo, un sistema de protección de datos más convencional, que no realiza la gestión de derechos de acceso. El método reivindicado se aplica entonces al suministro de los mensajes necesarios para el enrutamiento de las claves de descifrado, por ejemplo.

En otra forma de realización, todos los segmentos de un bloque de segmentos de contenido no se siguen inmediatamente en el desarrollo temporal del contenido. Algunos de estos segmentos están separados por segmentos que no pertenecen al bloque considerado.

Como una variante, un terminal comparte con al menos otro terminal su clave de cifrado y su clave de descifrado, denominadas de terminal.

En una variante, la red 3 comprende una primera subred de transmisión unidireccional de informaciones entre la cabecera de red 1 y el terminal 4, y una segunda subred para la transmisión bidireccional de informaciones entre el servidor 2 y el terminal 4. A modo de ejemplo, la primera subred es una red de transmisión por satélite y la segunda subred es la red de Internet.

Como alternativa, el reloj 12 de la cabecera de red 1 está sincronizado con un reloj de referencia, según un protocolo distinto de NTP. En otra variante, el reloj 12 está sincronizado con el servidor 2 de fechas. En otra variante, el reloj 12 está sincronizado con un reloj de referencia interno en la cabecera de red 1. En una última variante, el reloj 12 es en sí mismo un reloj de referencia interno en la cabecera de red 1. Del mismo modo, el servidor 2 de fechas puede estar sincronizado con un reloj de referencia según un protocolo distinto de NTP. En otra variante, el servidor 2 en sí mismo comprende un reloj de referencia con el que está sincronizado. También es posible que el reloj 12 y el servidor 2 de fechas, estén sincronizados con relojes de referencia según diferentes protocolos.

Como una variante, el servidor 2 de fechas está integrado con la cabecera de red 1.

La cantidad de bloques y segmentos por bloque puede variar. A modo de ejemplo, el flujo 6 tiene un solo bloque de segmentos de contenido. En otra variante, cada bloque incluye un solo segmento. En otra forma de realización, el número de segmentos en cada bloque no es necesariamente el mismo de un bloque a otro.

La fecha TS_i de transmisión del segmento 622 se puede insertar en un mensaje o una estructura de datos distinta de la licencia intermedia asociada a este segmento. Sin embargo, este mensaje u otra estructura de datos se transmite junto con el segmento y la licencia intermedia. A modo de ejemplo, la fecha de transmisión es adyacente a cada segmento transmitido en el flujo, pero no forma parte de la estructura de datos que constituye la licencia L_i.

Son posibles otras formas de realización de la licencia de L_p. Por ejemplo, la cabecera de red 1 puede, en la etapa 1200, para completar el derecho de acceso 52 de la licencia L_p, combinar reglas o criterios de acceso adicionales con el criptograma $(K_{Gp})*K_T$. En la etapa 1416, estas reglas o criterios adicionales se extraen entonces, asimismo, del derecho de acceso 52, por el terminal 4, y luego se evalúan. El éxito de esta evaluación condiciona la puesta en práctica de la etapa 1418 de descifrado del criptograma $(K_{Gp})*K_T$.

En una variante, la cabecera de red 1 obtiene la fecha de transmisión de un segmento desde el servidor 2 de fechas, o desde un servidor de fechas tercero, externo al sistema ilustrado en la Figura 1.

Como alternativa, el servicio de suministro de contenido considerado, es un servicio de difusión o de telecarga de contenidos, cuyo registro no está controlado por el sistema de protección de contenido, y la demanda recibida en la etapa 1100 es para obtener el contenido para guardarlo con el fin de reproducirlo más tarde. Las etapas 1204 y 1206 no responden a ninguna restricción de sincronización, por lo que, dependiendo de la dinámica del servicio, pueden ser simultaneadas o sucederse entre sí en cualquier orden. Sucede lo mismo con las etapas 1300 y 1302.

En otra realización alternativa, la duración predeterminada TSW no se utiliza. Lo anterior equivale a tomar esta duración TSW igual a cero en la etapa 1404 del método de la Figura 5. Asimismo, no es necesario utilizar la duración predeterminada ETTD. Por lo tanto, lo que antecede es equivalente a considerar que en la etapa 1404 de la Figura 5, la duración ETTD es infinita. En este caso, la actualización de la fecha TT_s se inicia de cualquier otro modo. A modo de ejemplo, esta actualización se inicia periódicamente, o después de recibir un número predeterminado de segmentos S_i a descifrar.

En una forma de realización alternativa, durante la etapa 1408, si el valor del contador de fallos de conexión supera el umbral Max_tts_bypass, el terminal 4 inhibe las etapas 1410 y siguientes del método, en particular, la extracción del derecho de acceso de la licencia L_p de terminal y, a modo de ejemplo, finaliza la fase de reproducción del contenido multimedia protegido.

En una realización alternativa, el terminal 4 no incluye un contador de fallos para la conexión al servidor 2 de fechas. Por lo tanto, en la etapa 1408, la primera vez que no puede establecerse la conexión con este servidor, el terminal inhibe la extracción del derecho de acceso de la licencia, lo que impide el acceso a los segmentos.

En la etapa 1414, si la última fecha de servicio adquirida TE no satisface el criterio temporal 54 de la licencia L_p encontrada en la etapa 1412, el terminal puede buscar o intentar utilizar otra licencia que incluya el identificador $Id(K_{Gp})$ 50 de la clave intermedia K_{Gp}. En otra forma de realización, inhibe las etapas 1416 y siguientes del método, en particular, la extracción del derecho de acceso de la licencia L_p de terminal, y finaliza, a modo de ejemplo, la fase de reproducción del contenido multimedia protegido.

REIVINDICACIONES

1. Método de suministro, a un terminal, de contenido multimedia protegido por un sistema de protección de contenidos multimedia, en donde:

durante una fase de emisión, una cabecera de red:

a) asocia (1200), a un bloque de segmentos de contenido multimedia, un derecho de acceso necesario para que el terminal acceda a cualquier segmento del bloque con miras a reproducirlo, y una licencia que incluye el derecho de acceso y un criterio temporal de validez, comprendiendo cada uno de dichos segmentos al menos una secuencia de grupos de imágenes de vídeo o de tramas de audio, incluyendo, dicho bloque, uno o más segmentos,

b) transmite (1204, 1206), al terminal la licencia y un flujo que incluye cada segmento,

durante una fase de recepción, el terminal:

c) recibe (1302) el flujo de segmentos de contenido multimedia;

d) recibe (1300) la licencia,

durante una fase de juego de los segmentos, el terminal:

e) autentifica (1408) un servidor de fechas y, solamente si el servidor de fechas es objeto de autenticación satisfactoria, adquiere (1408) una fecha de servicio a partir de este servidor de fechas,

f) evalúa (1414) el criterio temporal de la licencia con respecto a la última fecha de servicio adquirida, luego, si el resultado de la evaluación es positivo, extrae (1416, 1418) el derecho de acceso de la licencia, permitiendo, de este modo, el acceso a los segmentos y, en caso contrario, inhibe (1414), la extracción del derecho de acceso de la licencia prohibiendo así el acceso a los segmentos,

estando dicho método caracterizado por cuanto que:

- durante la etapa b), la cabecera de red asocia (1202) a cada uno de los segmentos, su fecha de transmisión, y la transmite (1206) en el flujo junto con el segmento, y luego, durante la fase de juego,

- en una etapa g), el terminal:

  - extrae (1400, 1402) del flujo, junto con un segmento, la fecha de transmisión del segmento, luego

  - compara (1404) la fecha de transmisión extraída con la última fecha de servicio adquirida, y

  - solamente si la fecha de transmisión extraída es posterior a esta última fecha de servicio adquirida, la adquiere (1406) como fecha de servicio, y la utiliza (1414) como última fecha de servicio adquirida en el momento de una próxima ejecución de la etapa f) entre dos ejecuciones sucesivas de la etapa e).

2. Método de obtención, por un terminal, para la puesta en práctica del método según la reivindicación 1, de contenidos multimedia protegidos, en donde el terminal:

en la fase de recepción:

- en la etapa c), recibe (1302) un flujo que comprende cada segmento del bloque de segmentos de contenido multimedia,

- en la etapa d), recibe (1300) una licencia que incluye un derecho de acceso necesario para que el terminal pueda tener acceso a cualquier segmento del bloque para poder reproducirlo, y un criterio temporal de validez,

en la fase de juego de los segmentos:

- en la etapa e), autentifica (1408) un servidor de fechas y, solamente si el servidor de fechas es objeto de autenticación de forma satisfactoria, adquiere (1408) una fecha de servicio a partir de este servidor de fechas,

- en la etapa f), evalúa (1414) el criterio temporal de validez de la licencia con respecto a la última fecha de servicio adquirida, luego, si el resultado de la evaluación es positivo, extrae (1416, 1418) el derecho de acceso de la licencia permitiendo así el acceso a los segmentos y, en caso contrario, inhibe (1414) la extracción del derecho de acceso de la licencia prohibiendo así el acceso a los segmentos,

estando el método caracterizado por cuanto que:

en la fase de juego, en la etapa g), el terminal:

- extrae (1400, 1402) del flujo, junto con un segmento, la fecha de transmisión de este segmento, luego
- compara (1404) la fecha de transmisión extraída con la última fecha de servicio adquirida, y
- solamente si la fecha de transmisión extraída es posterior a esta última fecha de servicio adquirida, la adquiere (1406) como fecha de servicio y la utiliza (1414) como última fecha de servicio adquirida en una siguiente ejecución de la etapa f) entre dos ejecuciones sucesivas de la etapa e).

3. Método según la reivindicación 2, en donde el derecho de acceso de la licencia comprende una clave intermedia o un criptograma de esta clave intermedia obtenido mediante el cifrado, con una clave criptográfica del terminal, siendo la clave intermedia una clave utilizada para cifrar las claves K_{si} de todos los segmentos del bloque de segmentos, siendo cada clave K_{si} la clave utilizada para cifrar un segmento respectivo del contenido multimedia.

4. Método según una cualquiera de las reivindicaciones 2 y 3, en donde el terminal, en la etapa g), compara la fecha de transmisión extraída con la última fecha de servicio adquirida y, solamente si la fecha de transmisión extraída es anterior a esta última fecha de servicio, en más de una primera duración predeterminada, entonces la última fecha de servicio adquirida se mantiene (1404) sin cambios, y la etapa f) se ejecuta utilizando esta última fecha de servicio adquirida que se ha mantenido sin cambios.

5. Método según una cualquiera de las reivindicaciones 2 a 4, en donde el terminal, en la etapa g), compara (1406) la fecha de transmisión extraída con la fecha de servicio adquirida durante la última ejecución de la etapa e), e inicia (1406) una nueva ejecución de la etapa e) si la diferencia entre la fecha de transmisión extraída y esta fecha de servicio es superior a una segunda duración predeterminada y, en caso contrario, no inicia (1406) esta nueva ejecución de la etapa e) en respuesta a esta comparación.

6. Método según una cualquiera de las reivindicaciones 2 a 5, en donde, en la etapa e), si no se puede establecer la conexión con el servidor de fechas, en respuesta, el terminal inhibe (1408) la extracción del derecho de acceso de la licencia prohibiendo así el acceso a los segmentos.

7. Método según la reivindicación 6, en donde:

- el terminal cuenta (1408) el número de veces consecutivas en las que no se puede establecer la conexión con el servidor de fechas, y
- en respuesta a la superación por este número de un umbral predeterminado, inhibe (1408) la extracción del derecho de acceso de la licencia prohibiendo así el acceso a los segmentos y, en caso contrario, autoriza (1408) la extracción del derecho de acceso de la licencia, autorizando así el acceso a los segmentos.

8. Método según una cualquiera de las reivindicaciones 2 a 7, en donde, entre dos ejecuciones consecutivas de la etapa f), el terminal extrae (1402) una o más fechas de transmisión de segmentos recibidas y, en cada extracción de una fecha de transmisión posterior a la última fecha de servicio adquirida, el terminal la adquiere (1406) como fecha de servicio, para ser utilizada como la última fecha de servicio adquirida en la siguiente realización de la etapa f).

9. Soporte de registro de informaciones, caracterizado por cuanto que incluye instrucciones para la puesta en práctica de un método conforme a una cualquiera de las reivindicaciones 2 a 8, cuando estas instrucciones son ejecutadas por ordenador.

10. Un terminal (4) para la puesta en práctica de un método de obtención de contenido multimedia de conformidad con una cualquiera de las reivindicaciones 2 a 8, en donde el terminal es capaz de:

en una fase de recepción:

c) la recepción de un flujo que comprende cada segmento de un bloque de segmentos de contenido multimedia, incluyendo cada uno de estos segmentos al menos una serie de grupos de imágenes de vídeo o de tramas de audio,

d) la recepción de una licencia que incluye un derecho de acceso necesario para que el terminal acceda a cualquier segmento del bloque para poder reproducirlo, y un criterio temporal de validez,

en una fase de juego de los segmentos:

e) la autenticación de un servidor de fechas y, solamente si el servidor de fechas fue autenticado de forma satisfactoria, la adquisición de una fecha de servicio a partir de este servidor de fechas,

f) la evaluación del criterio temporal de validez de la licencia con respecto a la última fecha de servicio adquirida, luego, si el resultado de la evaluación es positivo, la extracción del derecho de acceso de la licencia, permitiendo así el acceso a los segmentos y, en caso contrario, inhibir la extracción del derecho de acceso de la licencia prohibiendo así el acceso a los segmentos,

estando el terminal caracterizado por cuando que comprende un ordenador (44) programado para, en la fase de juego, poner en práctica una etapa g) en donde:

- extrae del flujo, junto con un segmento, la fecha de transmisión de este segmento, luego
- compara la fecha de transmisión extraída con la última fecha de servicio adquirida, y
- solamente si la fecha de transmisión extraída es posterior a esta última fecha de servicio adquirida, la adquiere como fecha de servicio y la utiliza como la última fecha de servicio adquirida en una siguiente ejecución de la etapa f) entre dos ejecuciones sucesivas de la etapa e).

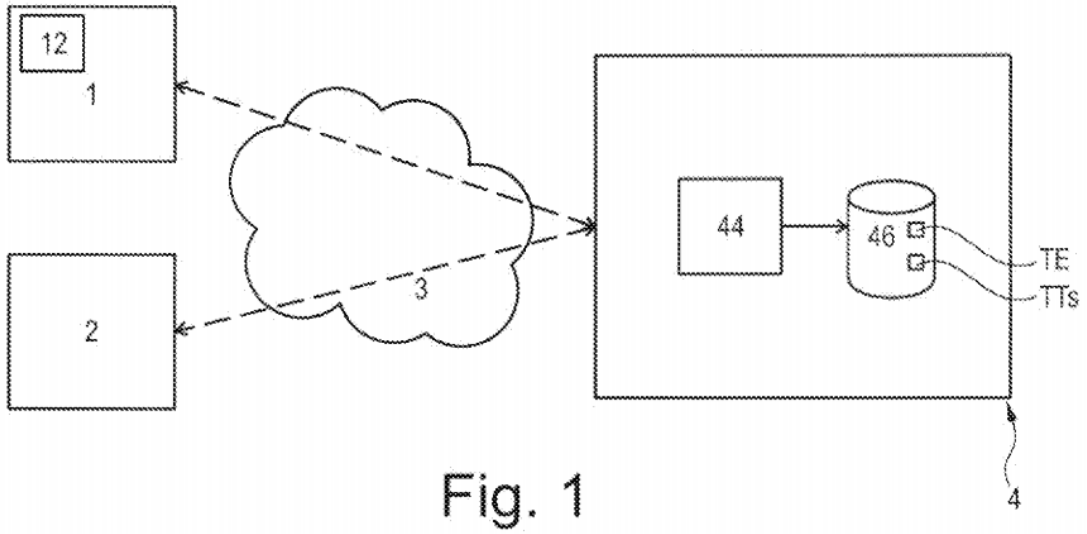

Fig. 1

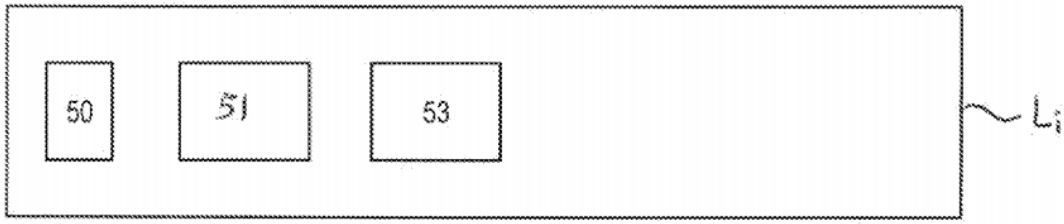

Fig. 2

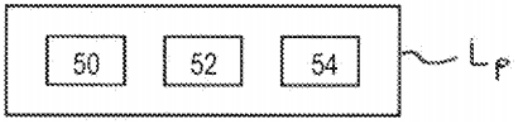

Fig. 3

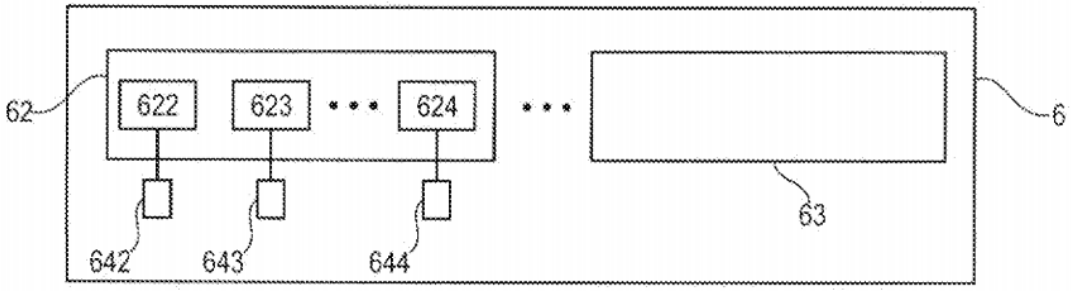

Fig. 4

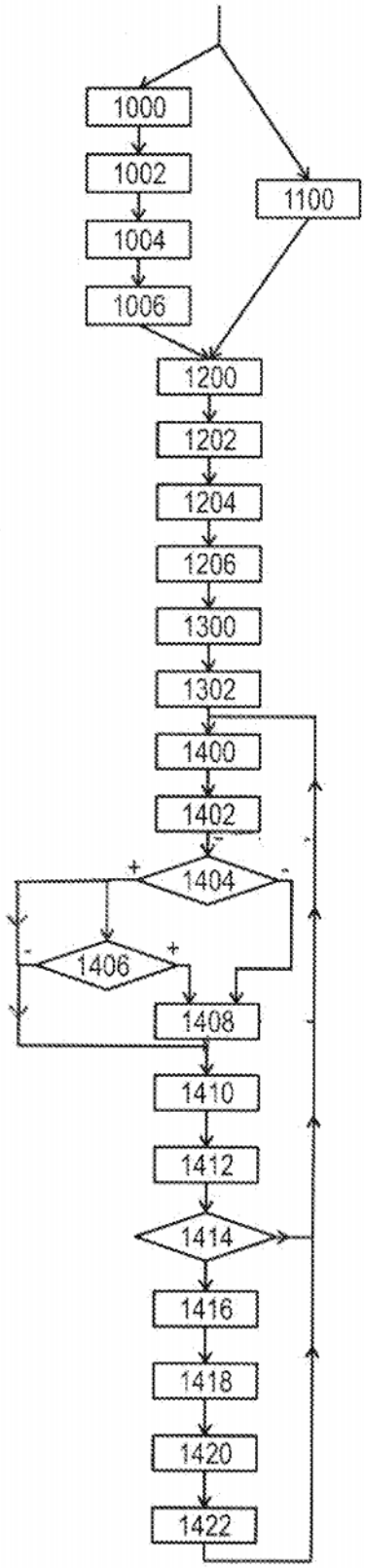
1000
1002
1004
1006
1100
1200
1202
1204
1206
1300
1302
1400
1402
1404
1406
1408
1410
1412
1414
1416
1418
1420
1422

Fig. 5