(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 394 767**

(51) Int. CI.:

H04N 21/418 (2011.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **24.06.2010 E 10167198 (0)**

(97) Fecha y número de publicación de la solicitud europea: **12.01.2011 EP 2273786**

(54) Título: **Control del acceso a un contenido digital**

(30) Prioridad:

26.06.2009 FR 0954372

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
05.02.2013

(73) Titular/es:

FRANCE TELECOM (100.0%)
6 place d'Alleray
75015 Paris, FR

(72) Inventor/es:

GUIONNET, CHANTAL y
FEVRIER, PIERRE

(74) Agente/Representante:

PÉREZ BARQUÍN, Eliana

DESCRIPCIÓN

Control del acceso a un contenido digital

La invención se refiere al dominio de la transmisión de contenidos multimedia en unas redes de transmisión y, más particularmente, al control del acceso a estos contenidos multimedia.

Las redes de transmisión de contenidos multimedia se pueden utilizar especialmente para las aplicaciones de televisión de pago.

En este tipo de redes de transmisión, se transmiten unos contenidos multimedia de manera cifrada y no se pueden restituir en un terminal receptor más que en ciertas condiciones. En efecto, el acceso a estos contenidos multimedia se controla generalmente en función de derechos de acceso y de criterios de acceso.

En un contexto de ese tipo, un terminal recibe sus derechos por medio de un mensaje único, que le está destinado individualmente. Un mensaje de ese tipo puede ser un mensaje inicial de derechos del tipo EMM (del inglés “Entitlement Management Message”). Este tipo de mensaje es un mensaje personalizado que se puede emitir destinado a un único abonado o incluso destinado a un grupo de abonados.

Posteriormente, en función de sus propios derechos cada terminal de la red de transmisión puede acceder o no a ciertos contenidos digitales. En efecto, por un lado el contenido digital se transmite de manera cifrada con ayuda de una clave de cifrado (o también CW de ‘Control Word’) y, por otro lado, la clave de cifrado se transmite en un mensaje sincronizado con la transmisión del contenido digital. De ese modo, con el fin de acceder al contenido digital, conviene descifrar en primer lugar la clave de cifrado que tiene asociada y que se recibe en un mensaje de control de acceso, por ejemplo del tipo ECM (del inglés “Entitlement Control Message”), sincronizado con un flujo de datos que transportan el contenido digital. El primer descifrado se puede realizar si el terminal dispone previamente de la clave de explotación que le permita descifrar este contenido digital. Esta clave de explotación está incluida en los derechos que el terminal ha recibido por medio del mensaje del tipo EMM. En consecuencia, si los derechos del terminal le autorizan, por medio de la presencia de la clave de explotación, a descifrar la clave de cifrado recibida en asociación con el contenido digital, entonces está en condiciones de descifrar este contenido digital.

En estas condiciones, el control de acceso se efectúa sobre la base de los derechos de acceso atribuidos a cada terminal.

Por otro lado, para ciertas aplicaciones, o en ciertos sistemas de control de acceso, además de estos derechos de acceso, se prevé controlar el acceso a un contenido digital sobre la base complementaria de criterios de acceso. Cumplir estos criterios de acceso puede corresponder por ejemplo a verificar si una suscripción específica está presente y válida. O incluso en verificar si una cuenta de usuario del terminal está suficientemente llena para poder pagar el acceso a un contenido cuyo coste, o débito a efectuar, constituye el criterio de acceso.

De ese modo, se puede autorizar a un terminal a acceder al contenido digital si, por un lado sus derechos le permiten descifrar el contenido digital recibido y, por otro lado, si se satisfacen los criterios de acceso a este contenido digital. Estos criterios de acceso se transmiten en unos mensajes del tipo ECM de manera síncrona con el flujo de datos correspondiente. Esta sincronización se requiere en un contexto de comunicación “one-to-many” es decir de una comunicación desde un origen hacia una pluralidad de receptores. Se puede tratar de una comunicación del tipo “broadcast” o “multicast”, por ejemplo.

En este contexto, los derechos de acceso transmitidos en unos mensajes EMM, se pueden individualizar por abonado, mientras que los criterios de acceso, transmitidos en los mensajes ECM de difusión general, son comunes a todos los abonados.

La figura 1 ilustra un sistema de difusión de contenidos digitales de acceso controlado de acuerdo con la técnica anterior.

Un sistema de ese tipo comprende una o varias entidades de gestión de los derechos de acceso 11, una entidad de transmisión de contenido digital 14 y unos terminales 12 y 15. La entidad de gestión de los derechos 11 transmite al terminal 12 un mensaje inicial de derechos EMM 101 que le transmite sus propios derechos A y al terminal 15 un mensaje inicial de derechos EMM 102 que le transmite sus propios derechos B.

Posteriormente, la entidad de transmisión 14 difunde de manera general 104 un contenido digital hacia los terminales del sistema 12 y 15. De manera síncrona con esta difusión general, se transmiten unos mensajes ECM 110 de control de derechos de acuerdo con la misma difusión general. Estos mensajes indican unos criterios de acceso comunes a todos los terminales destinatarios de la difusión general.

El documento EP 2.063.638 divulga una gestión de derechos de acceso a un contenido digital difundido. Un terminal STB comprende un módulo de control de acceso y un módulo de seguridad. El módulo de seguridad almacena unos

derechos del usuario que se reciben mediante unos mensajes del tipo EMM. Estos derechos Di se almacenan en una tabla de derechos Td que incluye igualmente unos índices de los indicadores del derecho ID.

El documento FR 2.843.468 divulga una difusión de contenido digital con control de acceso para hacer unas ofertas de compra. En este contexto se utilizan unos mensajes de control del tipo ECM. Se transportan unos criterios de acceso mediante estos mensajes de control.

La presente invención trata de mejorar la situación.

Un primer aspecto de la presente invención propone un procedimiento de gestión del control de acceso de al menos un contenido digital en función de al menos un criterio de acceso, siendo transmitido dicho contenido digital a al menos un terminal en la forma de un flujo de datos;
en el que dicho criterio acceso se almacena en función de un identificador en relación con el terminal;
comprendiendo dicho procedimiento las etapas siguientes, en dicho terminal:

/a/ recibir el flujo de datos en asociación con un mensaje que indica dicho identificador;
/b/ recuperar el criterio de acceso en la memoria en función del identificador recibido en el mensaje de control; y
/c/ verificar si el criterio de acceso almacenado se satisface con el fin, llegado el caso, de autorizar el acceso al contenido.

Se entiende por el término “terminal” todo tipo de terminal adaptado para recibir un flujo de datos que corresponde a la transmisión de un contenido digital. Un terminal de ese tipo puede ser un aparato de televisión, un ordenador, un teléfono móvil, etc…

Se entiende por la expresión “criterios de acceso” todo criterio que se pueda tener en cuenta en el terminal con el fin de autorizar o de prohibir un acceso al contenido digital recibido en función de derechos individuales del terminal. Un criterio de acceso de ese tipo puede corresponder especialmente a un tipo de suscripción. Se puede prever en efecto que un contenido no pueda estar accesible más que a los terminales que hayan suscrito una suscripción específica asociada con este contenido digital. Se puede prever igualmente un coste a pagar por terminal para el acceso a un contenido digital, por ejemplo en las aplicaciones de televisión del tipo PPV (de “Pay Per View”). En este caso, un terminal satisface el criterio de acceso si el crédito de que dispone es superior al coste que representa el acceso al contenido digital. Gracias a las presentes características, es posible que el coste del acceso al contenido digital sea diferente en función del terminal considerado. Por ejemplo, se puede desear hacer pagar un precio menor por el acceso al contenido digital a un terminal que por otro lado sea un gran “consumidor” de contenidos digitales. Es posible igualmente aplicar un modo de realización de la presente invención para efectuar un control parental o un control por dirección geográfica y de ese modo filtrar ciertos contenidos para ciertos terminales.

Se entiende por las expresiones “contenido digital” todo contenido que se pueda transmitir a través de una red de transmisión, tal como un contenido de audio, un contenido visual, un contenido audiovisual o más generalmente multimedia.

Los criterios de acceso se pueden individualizar fácilmente de ese modo, permitiendo así una gran flexibilidad de ofertas posibles de suministro de contenidos digitales.

No está ligada a la presente invención ninguna limitación en relación con el tipo de transmisión utilizada para transmitir el flujo de datos. Se puede concebir por ejemplo una difusión general del flujo de datos. En este caso, un modo de realización de la presente invención se puede implementar simplemente en un sistema de control de acceso al contenido digital de la técnica anterior.

Gracias a estas características, es posible transmitir a un terminal, en una red de transmisión de contenido digital, unos criterios de acceso que le sean propios, optimizando además la utilización de la banda pasante en la red de transmisión utilizada. En efecto, conviene observar que solamente se transmite un identificador en asociación con el flujo de datos y no criterios de acceso que podrían, por sí mismos, ocupar una banda pasante más grande, y tanto más si se desea personalizar los criterios de acceso en un contexto de difusión general. Este aspecto es tanto más ventajoso cuando el mensaje considerado se repite frecuentemente. Este es especialmente el caso cunado el mensaje considerado es un mensaje del tipo ECM que transporta también las CW, como en un contexto de difusión del tipo TV en directo, para el que las CW se debe modificar regularmente. En este tipo de contexto, los mensajes considerados se repiten frecuentemente y el hecho de que sean más cortos permite una ganancia perceptible de la banda pasante.

Por otro lado, la transmisión de un identificador único, que puede ser común a todos los terminales de la red para un contenido digital dado, permite ventajosamente individualizar los criterios de acceso por terminal, puesto que este identificador apunta a unos criterios de acceso almacenados en cada terminal, pudiendo ser estos criterios de acceso diferentes según los terminales de la red. Se realiza de ese modo la individualización de los criterios de acceso mientras se reduce la ocupación de la banda pasante de la red.

Se prevé en este caso almacenar en el terminal un criterio de acceso o una lista de criterios de acceso en asociación con un identificador. Este identificador permite apuntar en la memoria a los criterios de acceso propios a cada terminal incluso en relación con cada uno de estos terminales.

De ese modo, transmitiendo este identificador en asociación con el flujo de datos, se está en posición de indicar al terminal unos criterios de acceso que le son propios para acceder al contenido digital que recibe, aunque la transmisión de este identificador se efectúe por difusión general, o por multidifusión. En efecto, en un contexto de ese tipo, se puede transmitir un mismo identificador a un grupo de terminales o incluso a todos los terminales de la red, mientras se asocia, en los terminales en sí, a unos criterios de acceso que son propios para cada uno de los terminales.

En un modo de realización de la presente invención, sólo se transmite un identificador en un mensaje asociado al flujo de datos, en lugar de la transmisión de una lista eventual de criterios de acceso. En consecuencia, los mensajes asociados con la transmisión del flujo de datos son en sí mismos reducidos, lo que permite una utilización optimizada de la banda pasante en la red de transmisión. Procediendo de ese modo, es posible generar los criterios de acceso de manera individualizada por terminal, mientras se reduce la saturación de la banda pasante en la red de transmisión.

El identificador asociado con un criterio de acceso o incluso con una lista de criterios de acceso propios de un terminal, puede corresponder a un flujo de datos digital dado. Cuando el identificador se transmite de manera sincronizada con el flujo de datos, de acuerdo con una difusión general, todos los terminales que deseen acceder a este contenido digital reciben el mismo identificador en unos mensajes asociados con el flujo de datos. Sin embargo, para cada uno de estos terminales, este identificador común recibido no está forzosamente asociado a los mismos criterios de acceso. De ese modo, incluso utilizando una difusión general, los criterios de acceso se pueden personalizar por terminal.

Se puede por lo tanto prever, en un modo de realización de la presente invención, que los identificadores se transmitan en unos mensajes del tipo ECM, de manera síncrona con el flujo de datos.

No está ligada ninguna limitación con el medio utilizado por el terminal para almacenar el o los criterios de acceso en función de un identificador. Se puede especialmente prever que el terminal reciba esta asociación de identificador con unos criterios de acceso y la recupere desde un soporte de almacenamiento como una llave USB por ejemplo o incluso mediante la recepción de un mensaje inicial previamente a la recepción del flujo de datos que transporta el contenido digital.

De ese modo, en un modo de realización, el procedimiento comprende además las etapas siguientes antes de la etapa /a/:

/i/ recibir un mensaje inicial que indique al menos el criterio de acceso y el identificador asociado a dicho criterio de acceso; y
/b/ almacenar dicho criterio de acceso en asociación con dicho identificador.

Un mensaje inicial de ese tipo se puede transmitir de manera individual al terminal. Se puede prever así transmitirle un mensaje inicial de derechos del tipo EMM.

En el modo de realización de la presente invención, el contenido digital se transmite en forma cifrada y el mensaje de control, que indica el identificador, indica además una clave de cifrado de dicho contenido digital.

En este caso, el mensaje de control puede corresponder a un mensaje del tipo ECM. Se puede enviar regularmente para garantizar una renovación de la clave de cifrado, modificada por razones de seguridad. Puede además enviarse más regularmente, incluso durante un período en el que la clave de cifrado del contenido digital no ha sido modificada. En efecto, estas repeticiones de los mensajes de control permiten reducir el tiempo de espera de un usuario del terminal en caso de petición de un nuevo contenido digital. Cuando el contenido digital corresponde a un programa de televisión, estas repeticiones de envío de mensajes de control que indica una misma clave de cifrado, permite reducir el tiempo de espera durante un cambio de cadena de televisión o incluso “zapping”.

Un segundo aspecto de la presente invención propone un procedimiento de gestión del control de acceso a al menos un contenido digital en función de al menos un criterio de acceso, siendo transmitido el contenido digital a al menos un terminal en la forma de un flujo de datos;
en el que dicho criterio de acceso se almacena en función de un identificador en relación con el terminal;
comprendiendo dicho procedimiento la etapa siguiente, en el ámbito de una entidad de gestión del control de acceso:

/i/ transmitir al menos un mensaje de control en asociación con el flujo de datos, indicando dicho mensaje de control dicho identificador.

En este caso, un terminal almacena una asociación entre un identificador y uno o varios criterios de acceso. De ese modo, la entidad de gestión del control de acceso transmite únicamente el identificador en asociación con el flujo de datos que corresponde al contenido digital considerado. Posteriormente, a continuación, el terminal está en condiciones de recuperar desde sí mismo los criterios de acceso que se deben satisfacer para acceder a este contenido digital. Se considera que los criterios de acceso se satisfacen en base a los derechos de acceso recibidos previamente. El mensaje de control que indica este identificador puede corresponder a un mensaje del tipo ECM.

En un modo de realización de la presente invención, antes de la etapa /i/, se efectúa en la etapa siguiente:

- transmitir un mensaje inicial al terminal, indicando dicho mensaje inicial un identificador asociado a dicho criterio de acceso.

En un modo de realización de la presente invención, el mensaje inicial corresponde un mensaje del tipo EMM que se puede enviar de manera individual a un terminal. Se puede prever o bien agrupar este identificador y los criterios asociados con los derechos de acceso en un mismo mensaje del tipo EMM, o bien incluso transmitir con este fin dos mensajes distintos. En cualquier caso, estos mensajes se pueden emitir destinados a un único terminal o incluso a un grupo de terminales.

De ese modo, con la recepción de un mensaje inicial, el terminal almacena la asociación entre el identificador y los criterios de acceso. Es suficiente a continuación no transmitir más que el identificador de manera agrupada, o bien en multidifusión o bien incluso en difusión general, a una pluralidad de terminales. Ventajosamente, se puede utilizar un único identificador por flujo de datos transmitidos, correspondiendo cada identificador a unos criterios propios en el terminal, en unas memorias respectivas.

En un modo de realización de la presente invención, el contenido digital se transmite en forma cifrada y el mensaje de control indica además una clave de cifrado del contenido digital. Este mensaje se puede transmitir regularmente en el tiempo, para permitir un tiempo reducido de cambio de acceso a un contenido digital. Cuando se prevé modificar la clave de cifrado, este mensaje de control se transmite de manera síncrona con el flujo de datos.

Un tercer aspecto de la presente invención propone un terminal que comprende unos medios adaptados para la implementación de un procedimiento de gestión del control de acceso de acuerdo con el primer aspecto de la presente invención.

Un cuarto aspecto de la presente invención propone una entidad de gestión del control de acceso que comprende unos medios adaptados para la implementación de un procedimiento de gestión del control de acceso de acuerdo con el segundo aspecto de la presente invención.

Esta entidad de gestión del control puede estar a cargo igualmente de generar la asignación de los derechos de acceso propios de cada terminal.

Un quinto aspecto de la presente invención propone una entidad de transmisión de contenido digital con control de acceso que comprende unos medios adaptados para la implementación de un procedimiento de gestión del control de acceso de acuerdo con el primer aspecto de la presente invención.

En un modo de realización, la entidad de transmisión y la entidad de gestión del control están localizadas conjuntamente.

Un sexto aspecto de la presente invención propone un sistema de control de acceso a un contenido digital, que comprende una entidad de gestión del control de acceso de acuerdo con el cuarto aspecto de la presente invención, una entidad de transmisión de contenido digital de acuerdo con el quinto aspecto de la presente invención y al menos un terminal de acuerdo con el tercer aspecto de la presente invención.

Un séptimo aspecto de la presente invención propone un programa de ordenador que comprende unas instrucciones para la implementación del procedimiento de acuerdo con el primer aspecto de la presente invención, cuando este programa se ejecuta por un procesador.

Un octavo aspecto de la presente invención propone un programa de ordenador que incluye unas instrucciones para la implementación del procedimiento de acuerdo con el segundo aspecto de la presente invención cuando este programa se ejecuta por un procesador.

Un noveno aspecto de la presente invención propone un mensaje de control de acceso a un contenido digital, en función de al menos un criterio de acceso, siendo transmitido dicho contenido digital a al menos un terminal en la forma de un flujo de datos;

dicho mensaje de control indica un identificador relativo al flujo de datos, estando asociado dicho identificador a dicho criterio de acceso.

Surgirán otras particularidades y ventajas de la presente invención en la descripción detallada a continuación, realizada con referencia a los dibujos adjuntos en los que:

- la figura 1 ilustra un sistema de control de acceso de acuerdo con la técnica anterior que ya se ha descrito anteriormente en el presente documento;
- la figura 2 ilustra las principales etapas del procedimiento de gestión del control de acuerdo con un modo de realización de la presente invención;
- la figura 3 ilustra un sistema de control de acceso de acuerdo con un modo de realización de la presente invención;
- la figura 4 ilustra un terminal de acuerdo con un modo de realización de la presente invención;
- la figura 5 ilustra una entidad de gestión del control de acceso de acuerdo con un modo de realización de la presente invención; y
- la figura 6 ilustra una entidad de transmisión del contenido digital de acuerdo con un modo de realización de la presente invención.

Unas referencias idénticas designan unos objetos idénticos o similares de una figura a otra.

La figura 2 ilustra las principales etapas del procedimiento de gestión del control de acuerdo con un modo de realización de la presente invención, en relación con un terminal del sistema de control de acceso.

Un contenido digital, que puede ser un contenido multimedia, se transmite a través de una red de transmisión a al menos un terminal en la forma de un flujo de datos. No está ligada ninguna limitación a la red de transmisión utilizada para esta transmisión de contenido digital.

En un ejemplo particular de realización, que no es en absoluto limitativo, los contenidos digitales son unos programas de televisión transmitidos en el modo “en directo” (es decir en tiempo real, en vivo), la red de transmisión es la Internet y el terminal comprende un decodificador de TV (TV de TeleVisión), igualmente denominado STB (Set Top Box).

Se almacenan previamente un o unos criterios de acceso en asociación con un identificador en relación con el terminal. Se puede prever el hacer corresponder un identificador a un contenido digital o incluso a una pluralidad de contenidos digitales. Este aspecto permanece ventajosamente flexible.

En el terminal, en una etapa 21, se recibe el contenido digital en la forma de un flujo de datos cifrado al que se asocia un mensaje de control que indica un identificador.

A continuación, en una etapa 22, se recupera el criterio de acceso o los criterios de acceso en la memoria en función del identificador recibido en el mensaje. A continuación, en una etapa 23, se controla si el o los criterios de acceso se satisfacen en base a un análisis de los derechos presentes. Finalmente, en una etapa 24, si el o los criterios de acceso se satisfacen, se decide entonces acceder al contenido digital recibido en el flujo de datos.

En un sistema de control de acceso de acuerdo con un modo de realización de la presente invención, el flujo de datos se transmite de acuerdo con una difusión general a todos los terminales y el mensaje de control asociado se transmite igualmente de manera síncrona en el flujo de datos. De ese modo, el identificador se relaciona con un contenido digital. Los criterios de acceso almacenados previamente en cada terminal pueden ser propios ventajosamente de cada uno de los terminales.

Un mensaje de control puede corresponder a un mensaje del tipo ECM y por tanto ser transmitido de manera síncrona con el contenido digital. Se puede indicar por tanto, además del identificador, punteros hacia unos criterios de acceso propios de cada terminal, la clave de cifrado asociada al contenido digital se transmite en una forma cifrada.

Se puede prever en un sistema de gestión del control de acceso que una entidad de gestión del control de acceso esté a cargo de transmitir a cada terminal de manera personal o incluso agrupada, una asociación entre un identificador y unos criterios de acceso, y una entidad de transmisión del flujo que, en sí, está encargada de difundir el contenido en la forma de un flujo de datos, al que se sincroniza un mensaje de control que indica especialmente el identificador que corresponde a este flujo de datos. Este mensaje de control se puede repetir ventajosamente en el transcurso del tiempo durante la difusión del flujo de datos.

La figura 3 ilustra un sistema de control de acceso de un contenido digital de acuerdo con un modo de realización de la presente invención.

Un sistema de control de acceso de ese tipo comprende una entidad de transmisión 34 del contenido digital en la forma de un flujo de datos a través de una red de transmisión, de acuerdo con un modo de realización.

Comprende además una entidad de gestión del control de acceso 31 para cada uno de los terminales 12 y 15 usuarios del sistema. Estos derechos de acceso pueden ser una suscripción de un tipo dado para un periodo dado, una reserva de sesión particular, un número de fichas que permitan a continuación una compra impulsiva local, una clave de descifrado, etc…

Esta entidad de gestión del control de acceso 31 está adaptada para transmitir a cada uno de estos terminales sus derechos de acceso respectivos. Con este fin, emite unos mensajes 101 y 102 que indican respectivamente los derechos de acceso del terminal 12 y los derechos de acceso del terminal 15.

Estos mensajes 101 y 102 pueden ser unos mensajes del tipo EMM. De ese modo el mensaje inicial de derechos 101 con destino en el terminal 12 indica los derechos de acceso A del terminal 12 y el mensaje de derechos 102 con destino en el terminal 15 indica los derechos de acceso B del terminal 15. Estos derechos de acceso A y B se almacenan en los terminales respectivos.

Con el fin de que los terminales que utilizan este sistema de control de acceso reciban sus criterios de acceso y el identificador que tienen asociado, se puede concebir utilizar o bien los mismos mensajes 101 y 102 o bien incluso otros mensajes del mismo tipo. Se puede prever igualmente que esta asociación de un identificador con los criterios de acceso se obtenga en el terminal de una manera cualquiera, por ejemplo por transferencia de datos física por medio de una clave de almacenamiento.

En un ejemplo ilustrado en la figura 3, se transmiten unos criterios de acceso respectivos A' y B' de los terminales 12 y 15, a través de los mensajes iniciales respectivos 301 y 302. Se puede prever que una pluralidad de identificadores que corresponden a una pluralidad de contenidos digitales o una pluralidad de tipos de acceso se transmita en un mismo mensaje inicial o incluso en unos mensajes iniciales respectivos distintos.

Cualquiera que sea el método implementado, en un cierto estado del procedimiento de gestión del control, los terminales almacenan en memoria, como por ejemplo en una tarjeta de memoria, por un lado sus derechos de acceso, respectivamente A o B, y por otro lado sus criterios de acceso, respectivamente A' o B' en asociación con un identificador.

Posteriormente, cuando un terminal solicita cierto contenido digital, como por ejemplo un programa de televisión o incluso una película, recibe entonces el contenido digital difundido por la entidad de transmisión en la forma de un flujo de datos 310. A este flujo de datos se asocia un mensaje de control que indica un identificador que corresponde al flujo de datos. De ese modo, con la recepción de este identificador, cada terminal recupera sus propios criterios de acceso en la memoria.

El acceso al contenido es entonces función de unos criterios de acceso y de unos derechos de acceso.

En un ejemplo de aplicación, el terminal de un sistema de control de acceso de acuerdo con un modo de realización de la presente invención solicita la recepción de una cadena de televisión. Se desea que el acceso al programa difundido en esta cadena de televisión no sea posible más que con una suscripción dada para ciertos terminales y a la elección entre la lista de suscripciones para otros terminales (criterios de acceso). En este caso, el flujo de datos que transmite el contenido digital que corresponde al programa de televisión se asocia a un flujo de mensajes de control que indican cada uno un único identificador asociado. Si el terminal ha recibido previamente este identificador y los criterios asociados entonces estos son estos criterios personalizados los que se aplican y se verifican en relación a los derechos personales de cada terminal para permitir al terminal acceder al contenido digital correspondiente.

En otro ejemplo de aplicación, la presente invención se describe en su aplicación a un servicio de televisión en modo PPV (de "Pay Per View"). El terminal de un sistema de control de acceso de acuerdo con un modo de realización de la presente invención solicita la recepción de una película por ejemplo. Tiene en memoria la asociación del acceso a esta película con un criterio de acceso que representa el coste de esta película. El coste se puede expresar en número de fichas. Posteriormente, recibe el flujo de datos que corresponde a esta película y al menos un mensaje de control que implica el identificador. En este momento, recupera de la memoria el coste del acceso a esta película. Puede comparar entonces con una cuenta de fichas que indica su crédito (derecho de acceso) y de ese modo autorizar o prohibir el acceso a esta película. En este caso, conviene observar que se puede prever ventajosamente que el coste del acceso a una película puede depender del terminal, especialmente para ofrecer unas promociones a los clientes importantes.

La figura 4 ilustra un terminal de acuerdo con un modo de realización de la presente invención. Un terminal de ese tipo puede comprender:

- una memoria 41 adaptada para almacenar una asociación entre un identificador y al menos un criterio de acceso;
- una unidad de recepción 42 adaptada para recibir el flujo de datos en asociación con un mensaje de control que indica dicho identificador;

- una unidad de gestión de la memoria 43 adaptada para recuperar el criterio de acceso en la memoria en función del identificador recibido en el mensaje de control; y
- una unidad de decisión 44 adaptada para verificar si el criterio de acceso almacenado se satisface y, llegado el caso, autorizar el acceso al contenido recibido en el flujo de datos.

La figura 5 ilustra una entidad de gestión del control de acceso 50 de acuerdo con un modo de realización de la presente invención. Una entidad de gestión del control de acceso de ese tipo puede comprender:

- una unidad de transmisión 51 adaptada para transmitir un mensaje inicial al terminal, indicando dicho mensaje inicial una asociación de un identificador y dicho criterio de acceso.

La figura 6 ilustra una entidad de transmisión del contenido digital 60 de acuerdo con un modo de realización de la presente invención. Una entidad de transmisión de ese tipo puede comprender:

- una unidad de transmisión 61 adaptada para transmitir un flujo de datos que corresponde al contenido digital, en asociación con al menos un mensaje de control que indica dicho identificador.

En un modo de realización de la presente invención, el terminal tiene necesidad no solamente de la CW o palabra de control o clave de cifrado del contenido, recibida en un mensaje clásico del tipo ECM, sino también de una CW suplementaria, o clave de cifrado, que puede recibir ventajosamente en un mensaje del tipo EMM que transporta la asociación de un identificador con unos criterios de acceso, es decir el mensaje inicial. Se puede incrementar de ese modo el grado de seguridad del control.

Es posible igualmente que los mensajes del tipo ECM transporten, además de un identificador, unos criterios de acceso suplementarios. En este caso, se pueden combinar los criterios de acceso recuperados en base al identificador y los recibidos directamente en el mensaje ECM.

En una variante se puede prever también que los mensajes iniciales indiquen por sí mismos unos identificadores que apunten a otros criterios ya almacenados en la memoria del terminal considerado. En este caso, el control de acceso a un contenido se puede basar en una combinación de criterios de acceso recibidos en el mensaje inicial y también de criterios de acceso apuntados en la memoria por el identificador o los identificadores recibidos en el mensaje inicial.

En un ejemplo, se prevé hacer depender el acceso a un contenido digital por ejemplo de una suscripción 1 que se recibiría mediante un mensaje inicial de acuerdo con un modo de realización de la presente invención y de una suscripción 2 que se recibiría en un mensaje del tipo ECM de difusión general asociada al flujo de datos.

Sólo se han descrito de modo explícito anteriormente algunos ejemplos. Sin embargo, se permite una gran flexibilidad de propuestas y de combinaciones de propuestas gracias a las características de la presente invención.

REIVINDICACIONES

1. Procedimiento de gestión del control de acceso a al menos un contenido digital en función de al menos un criterio de acceso (A', B'), siendo transmitido dicho contenido digital a al menos un terminal (12, 15) en la forma de un flujo de datos;
en el que dicho criterio de acceso se almacena en memoria en asociación con un identificador (id) en relación con el terminal, siendo dicho identificador un puntero hacia dicho criterio de acceso;
comprendiendo dicho procedimiento las etapas siguientes, en el ámbito de dicho terminal:

/a/ recibir (21) el flujo de datos en asociación con un mensaje de control (304) que transmite dicho identificador;
/b/ recuperar (22) el criterio de acceso en la memoria en función del identificador recibido en el mensaje de control; y
/c/ verificar si el criterio de acceso almacenado se satisface con el fin, llegado el caso, de autorizar el acceso al contenido.

2. Procedimiento de gestión del control de acceso de acuerdo con la reivindicación 1, que comprende además las etapas siguientes antes de la etapa /a/:

/i/ recibir un mensaje inicial (301, 302) que transmite al menos el criterio de acceso (A', B') y el identificador (id) asociado a dicho criterio de acceso; y
/ii/ almacenar dicho criterio de acceso en asociación con dicho identificador.

3. Procedimiento de gestión del control de acceso de acuerdo con la reivindicación 1, en el que el contenido digital se transmite en forma cifrada (310) y el mensaje de control (304) indica además una clave de cifrado de dicho contenido digital.

4. Procedimiento de gestión del control de acceso a al menos un contenido digital en función de al menos un criterio de acceso (A', B') en relación con un terminal (12, 15),
en el que dicho criterio de acceso se almacena en asociación con un identificador (id) en relación con el terminal, siendo dicho identificador un puntero hacia dicho criterio de acceso;
comprendiendo dicho procedimiento la etapa siguiente, en el ámbito de la entidad de transmisión del flujo de datos:

- transmitir un flujo de datos (310) que corresponde al contenido digital, en asociación con al menos un mensaje de control (304) que transmite dicho identificador.

5. Procedimiento de gestión del control de acceso de acuerdo con la reivindicación 4, en el que el contenido digital se transmite en forma cifrada y el mensaje de control (304) indica además una clave de cifrado de dicho contenido digital.

6. Procedimiento de gestión del control de acceso a al menos un contenido digital en función de al menos un criterio de acceso (A', B') en relación con terminal (12, 15);
en el que dicho criterio de acceso se almacena en asociación con un identificador (id) en relación con el terminal, siendo dicho identificador un puntero hacia dicho criterio de acceso;
comprendiendo dicho procedimiento la etapa siguiente en el ámbito de una entidad de gestión del control de acceso (50):

- transmitir un mensaje inicial (301, 302) al terminal, transmitiendo dicho mensaje inicial una asociación de un identificador (id) y dicho criterio de acceso.

7. Terminal (12, 15) adaptado para acceder a un contenido digital de acuerdo con una gestión del control de acceso basada en al menos un criterio de acceso (A', B'), siendo transmitido dicho contenido digital a al menos un terminal en la forma de un flujo de datos (310);
comprendiendo dicho terminal:

- una memoria (41) adaptada para almacenar una asociación entre un identificador (id) y al menos un criterio de acceso, siendo dicho identificador un puntero hacia dicho al menos un criterio de acceso;
- una unidad de recepción (42) adaptada para recibir el flujo de datos en asociación con un mensaje de control (304) que transmite dicho identificador;
- una unidad de gestión de memoria (43) adaptada para recuperar el criterio de acceso en la memoria en función del identificador recibido en el mensaje de control; y
- una unidad de decisión (44) adaptada para verificar si el criterio de acceso almacenado se satisface y, llegado el caso, autorizar el acceso al contenido digital recibido en el flujo de datos.

8. Entidad de gestión del control de acceso (50) a al menos un contenido digital en función de al menos un criterio de acceso en relación con un terminal (12, 15);
en la que dicho criterio de acceso se almacena en asociación con un identificador (id) en relación con el terminal,

siendo dicho identificador un puntero hacia dicho criterio de acceso;
comprendiendo dicha entidad de gestión del control de acceso:

- una unidad de transmisión (51) adaptada para transmitir un mensaje inicial al terminal, transmitiendo dicho mensaje inicial una asociación de un identificador (id) y dicho criterio de acceso.

9. Entidad de transmisión del contenido digital (60) de acceso controlado en función de al menos un criterio de acceso (A', B') en relación con el terminal (12, 13), en el que dicho criterio de acceso se almacena en asociación con un identificador (id) en relación con el terminal, siendo dicho identificador un puntero hacia dicho criterio de acceso;
comprendiendo dicha entidad de transmisión:

- una unidad de transmisión (61) adaptada para transmitir un flujo de datos que corresponde al contenido digital, en asociación con al menos un mensaje de control (304) que transmite dicho identificador (id).

10. Sistema de control de acceso a un contenido digital, que comprende una entidad de gestión del control de acceso (50) de acuerdo con la reivindicación 8, una entidad de transmisión del contenido digital (60) de acuerdo con la reivindicación 9 y al menos un terminal (12, 15) de acuerdo con la reivindicación 7.

11. Programa de ordenador que incluye unas instrucciones para la realización del procedimiento de acuerdo con la reivindicación 1, cuando este programa se ejecuta por un procesador.

12. Programa de ordenador que incluye unas instrucciones para la realización del procedimiento de acuerdo con la reivindicación 4, cuando este programa se ejecuta por un procesador.

13. Mensaje de control de acceso (304) a un contenido digital, en función de al menos un criterio de acceso (A', B'), siendo transmitido dicho contenido digital a al menos un terminal (12, 15) en la forma de un flujo de datos (310);
siendo almacenado dicho criterio de acceso en asociación con un identificador (id) en relación con el terminal;
transmitiendo dicho mensaje de control dicho identificador (id) en relación al flujo de datos, estando asociado dicho identificador a dicho criterio de acceso y en el que es un puntero hacia dicho criterio de acceso.

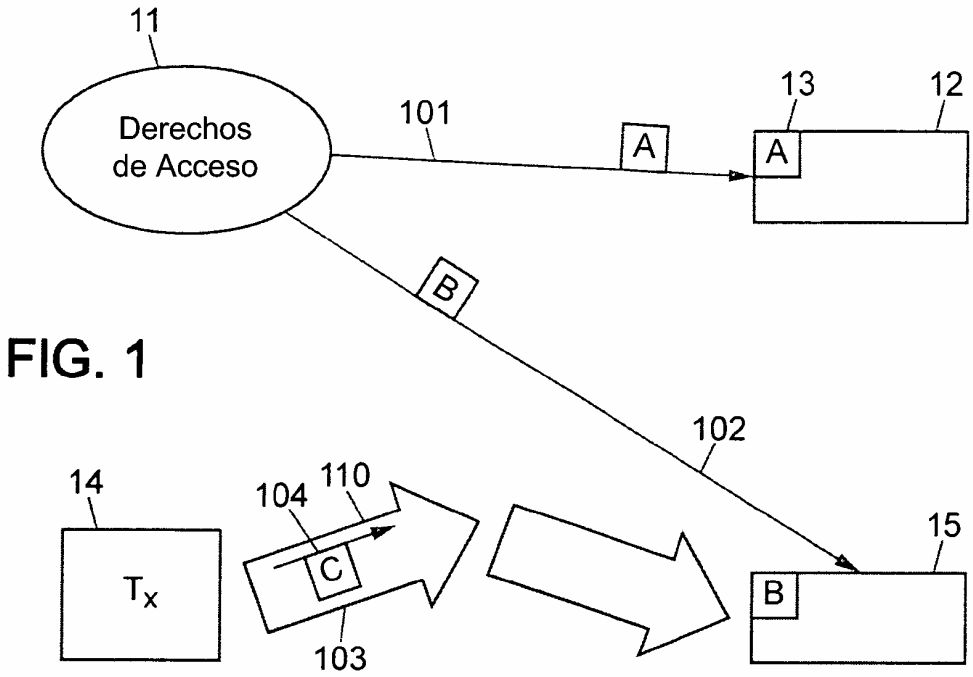
11
Derechos
de Acceso
101
A
13
12
A
B
102
14
104
110
C
15
T_x
B
103

FIG. 1

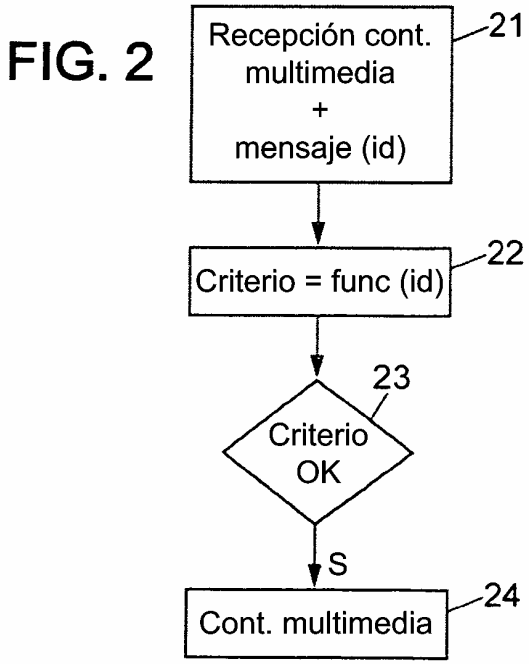
Recepción cont.
multimedia
+
mensaje (id)
21
Criterio = func (id)
22
23
Criterio
OK
S
Cont. multimedia
24

FIG. 2

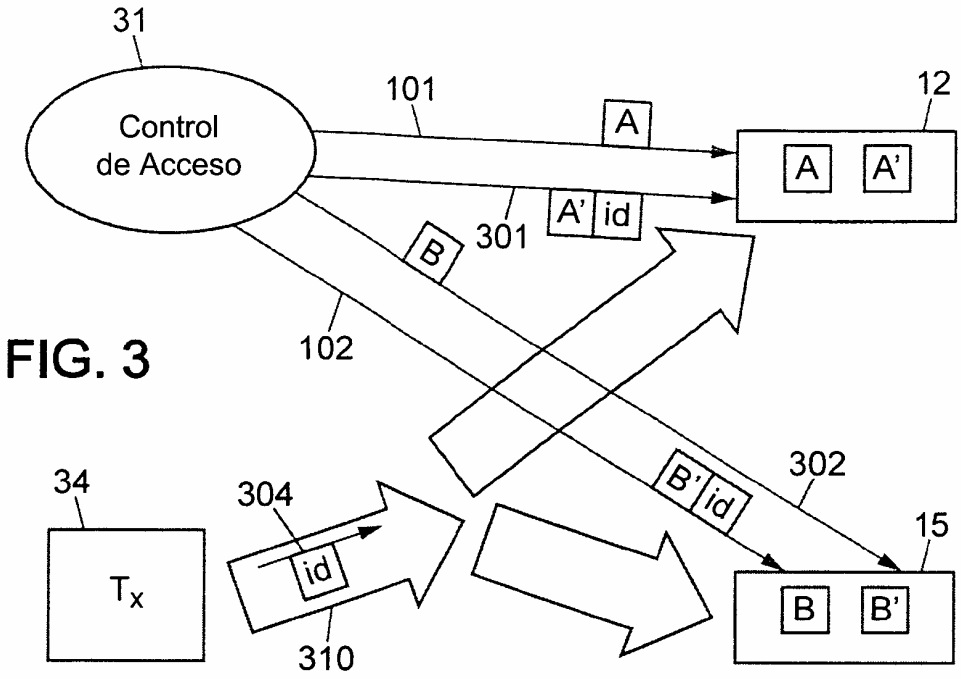
31
Control
de Acceso
101
A
12
A
A'
A'
id
301
B
102
302
B'
id
34
304
id
15
Tx
B
B'
310

FIG. 3

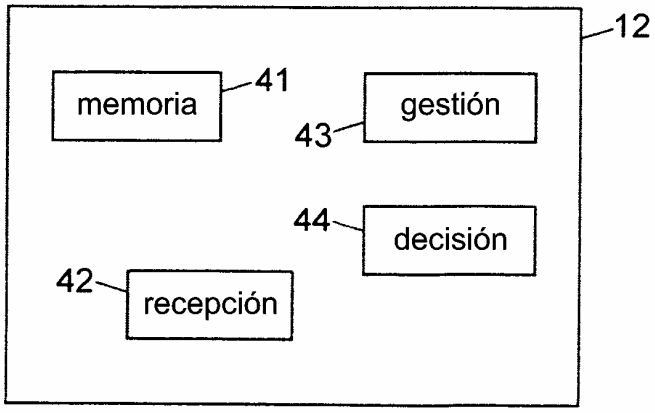
12
memoria
41
gestión
43
44
decisión
42
recepción

FIG. 4

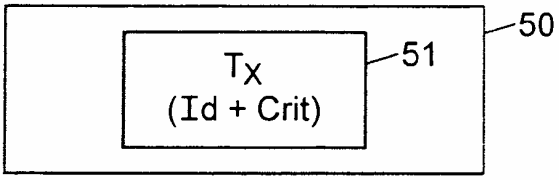

FIG. 5

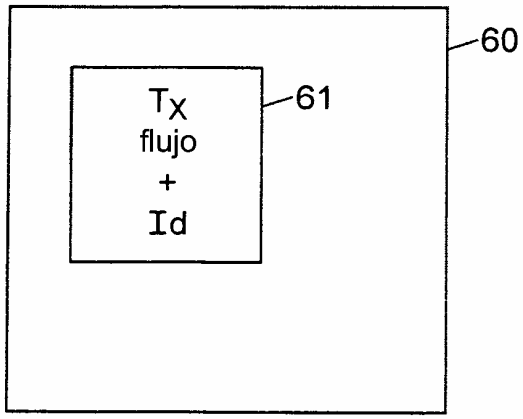

FIG. 6