(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 391 555**

(51) Int. CI.:
H04N 21/418 (2011.01)
H04N 21/4147 (2011.01)
H04N 21/4405 (2011.01)
H04N 21/4408 (2011.01)
H04N 21/426 (2011.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **03712576 .2**
(96) Fecha de presentación: **15.04.2003**
(97) Número de publicación de la solicitud: **1497986**
(97) Fecha de publicación de la solicitud: **19.01.2005**

(54) Título: **Método de gestión de derechos de un contenido cifrado y almacenado en una grabadora digital personal**

(30) Prioridad:
19.04.2002 CH 664022002

(45) Fecha de publicación de la mención BOPI:
27.11.2012

(45) Fecha de la publicación del folleto de la patente:
27.11.2012

(73) Titular/es:
NAGRAVISION SA (100.0%)
22, ROUTE DE GENEVE
1033 CHESEAUX-SUR-LAUSANNE, CH

(72) Inventor/es:
SASSELLI, MARCO

(74) Agente/Representante:
TOMAS GIL, Tesifonte Enrique

DESCRIPCIÓN

Método de gestión de derechos de un contenido cifrado y almacenado en una grabadora digital personal.

[0001] La presente solicitud se refiere al ámbito de los receptores/decodificadores de servicios con acceso condicionado, en particular de receptores que disponen de unidad de almacenamiento tales como los discos duros.

[0002] La evolución tecnológica en el ámbito de las capacidades de almacenamiento y de la rapidez de los discos magnéticos (disco duro) ha hecho que se haya hecho posible almacenar el contenido de video teletransmitido para ser accedido en diferido por el usuario.

[0003] Tales grabadoras son conocidas bajo la marca ReplayTV® o Tivo® y proponen almacenamientos de varias decenas de horas de transmisión digital. Estas grabadoras no están sin embargo directamente integradas en los receptores/decodificadores de servicios con acceso condicional; en particular, el contenido es almacenado sin protección particular sobre el disco, lo que hace imposible la recopilación de los derechos de autor asociados al contenido, en caso de que el disco fuera a continuación duplicado con el fin de una redistribución comercial. Además, el acceso al contenido

[0004] A la inversa, en un sistema de televisión digital de pago, el flujo digital transmitido hacia estos receptores se codifica con el fin de poder controlar la utilización y de definir las condiciones para tal utilización. Este cifrado se realiza gracias a palabras de control (Control Words) que se cambian en un intervalo regular (normalmente entre 5 y 30 segundos) con el fin de disuadir todo ataque dirigido a recobrar tal palabra de control.

[0005] Según un modo de realización particular, las palabras de control se cambian a intervalos mucho más largos lo que significa que para un evento considerado, se codifica por una sola palabra de control. Para que el receptor pueda descifrar el flujo cifrado por estas palabras de control, estos últimos se mandan independientemente del flujo en mensajes de control (ECM) cifrados por una clave propia del sistema de transmisión entre el centro de gestión (CAS) y el módulo de seguridad de la unidad de usuario. De hecho, las operaciones de seguridad se efectúan en una unidad de seguridad (SC) que está habitualmente bajo la forma de una tarjeta inteligente, considerada inviolable. Esta unidad puede ser o de tipo móvil o directamente integrada en el receptor.

[0006] En el momento de la descifrado de un mensaje de control (ECM), se verifica, en la unidad de seguridad (SC), que el derecho para acceder al flujo considerado está presente. Este derecho se puede gestionar a través de mensajes de autorización (EMM) que cargan un tal derecho en la unidad de seguridad (SC). Otras posibilidades son igualmente posibles tales como el envío de claves de descifrado.

[0007] Para la continuación de la exposición, se llamará "evento" a un contenido de video, audio (por ejemplo MP3) o datos (programa de juego por ejemplo) que se codifica según el método conocido por las palabras de control, cada evento pudiendo ser cifrado por una o una varias palabras de control, cada una teniendo un periodo de validez determinado.

[0008] La contabilización de la utilización de tales eventos está hoy basada en el principio del abono, de la compra de eventos o del pago por unidad de tiempo.

[0009] El abono permite definir un derecho asociado a uno o varios canales de difusión transmitiendo estos eventos y permite al usuario obtener estos canales en claro si el derecho está presente en su unidad de seguridad.

[0010] Paralelamente, es posible definir los derechos propios a un evento, como una película o un partido de fútbol. El usuario puede adquirir este derecho (compra por ejemplo) y este evento será específicamente gestionado por este derecho. Este método es conocido bajo la denominación "pay-per-view" (PPV).

[0011] Por cuanto concierne al pago por unidad de tiempo, la unidad de seguridad incluye un crédito que se entrega en función del consumo real del usuario. De este modo por ejemplo, una unidad será cargada cada minuto a este crédito según sea el canal o el evento mirado. Es posible según las implementaciones técnicas, variar la unidad de contabilización, sea en la duración, sea en el valor del tiempo concedido, incluso combinando estos dos parámetros para adaptar la facturación al tipo de evento transmitido.

[0012] Un mensaje de control (ECM) no contiene únicamente la palabra de control sino también las condiciones para que esta palabra sea devuelta al receptor/descodificador. En el momento de la descifrado de las palabras de control, será verificado si un derecho asociado a las condiciones de acceso enunciadas en el mensaje está presente en la unidad de seguridad.

[0013] La palabra de control no es devuelta a la unidad de usuario más que cuando la comparación es positiva. Esta palabra de control está contenida en un mensaje de control ECM que se codifica por una clave de transmisión TK.

[0014] Para que el derecho esté presente en la unidad de seguridad, es habitualmente cargado en esta unidad por un mensaje de gestión de derecho (EMM) que por razones de seguridad, es habitualmente cifrado por una clave diferente llamada clave de derecho (RK).

[0015] Según una forma conocida de difusión de televisión de pago, los tres elementos siguientes son necesarios para descifrar un evento en un momento dado:

- el evento cifrado por una o varias de palabras de control (CW),

- el o los mensajes de control ECM conteniendo las palabras de control (CW) y las condiciones de acceso (AC)

- el derecho correspondiente almacenado en la unidad de seguridad que permite verificar dichas condiciones de acceso.

[0016] Según un esquema conocido, el evento cifrado que se almacena en una unidad de almacenamiento tal como un disco duro, se acompaña al menos del o de los mensajes de control ECM.

[0017] Debido a que la descifrado a posteriori de los mensajes ECM puede suponer un problema, en particular a causa del cambio de la clave de transmisión, una primera solución es propuesta en el documento EP 0 912 052, solución que implica la descifrado de estos mensajes en la unidad de seguridad y el recifrado antes del almacenamiento sobre el disco. Esta solución es igualmente descrita en la solicitud EP 0 975 165.

[0018] Esta solución resuelve el problema de la duración de la vida de la clave de transmisión (cambio de claves) pero carga en gran medida la unidad de seguridad en el momento del registro, sin saber si el contenido grabado será algún día utilizado. Además, una de las reglas fundamentales del sistema de seguridad es devolver a la unidad de usuario las palabras de control sólo si los derechos existen. En tal caso, puede ser que estos derechos no existan si se considera una compra por evento. El derecho será adquirido en el momento de la compra que puede hacerse mucho más tarde del momento en el que el usuario decide visualizar este evento.

[0019] Este documento EP 0 912 052 no resuelve el problema del acceso al derecho porque en el momento de la compra, el mensaje de derecho EMM debe ser siempre difundido para que sea cargado en la unidad de seguridad.

[0020] De este modo, la solución descrita en este documento no es aplicable más que para unos eventos difundidos para los cuales el derecho está ya presente en la unidad de seguridad con el fin de autorizar la descifrado y el recifrado de los ECM.

[0021] Otro aspecto es la conservación de los derechos de un titular. Tomemos el ejemplo en el que un titular A dispone de los derechos de recepción de los canales M, N, P. Tiene por lo tanto el derecho de visualizar estos canales y por lo tanto de grabar y de visualizar a voluntad los eventos que se hallan sobre su unidad de almacenamiento. A cada utilización de un tal evento, la unidad de seguridad será requerida para descifrar los mensajes ECM y devolver las palabras de control. Es entonces importante que los derechos ligados a este evento estén presentes en la unidad de seguridad.

[0022] En el caso de un evento obtenido gracias a un abono, la identificación de este evento se asocia al canal del abono, por ejemplo M. De este modo todos los eventos que llevan el identificador M son autorizados y las palabras de control son devueltas al descodificador.

[0023] Estos derechos son por lo tanto asociados a un canal particular definido por un identificador como M. Cuando el abonado cancela su abono, o lo modifica por otros canales, resulta que los eventos grabados sobre la unidad de almacenamiento serán inaccesibles porque la unidad de seguridad se negará a devolver las palabras de control, el derecho correspondiente dejando de estar presente.

[0024] Esta situación puede producirse igualmente si el canal M se atribuye un nuevo identificador. Es de este modo posible que la reorganización de los canales haga que este canal se encuentre con el identificador J4 en lugar de M. Desde el punto de vista de los derechos de difusión, la unidad de seguridad es informada en tiempo útil y ningún desagrado es constatado por el usuario.

[0025] En cambio, las consecuencias para un evento grabado son más dramáticos. Esta reasignación tendrá sencillamente como consecuencia que el evento grabado será inaccesible porque el derecho correspondiente ya no está presente en la unidad de seguridad.

[0026] Un ejemplo de un tal dispositivo es descrito en la solicitud de patente europea EP 0 936 774. Este dispositivo está en particular destinado a recibir ficheros musicales. Cada fichero se asocia a una clave específica. Igualmente, cada dispositivo receptor dispone de su propia clave. Cuando el receptor solicita el envío de una pieza musical, el fichero correspondiente es codificado mediante la clave específica de esta pieza. La clave de la pieza es a continuación enviada al receptor en forma codificada por la clave del receptor.

[0027] En este dispositivo, mientras que la clave del receptor no cambie, los ficheros memorizados en este receptor son accesibles. En cambio, desde que hay un cambio de clave, los ficheros dejan de ser accesibles. Este dispositivo no asegura por lo tanto la perennidad del acceso a los ficheros en caso de cambio de parámetros ligados al sistema.

[0028] El objetivo de la presente invención es proponer un método de almacenamiento de un evento cifrado por palabras de control (CW) que garantiza el acceso a este evento en cualquier momento, aunque ciertas modificaciones en la designación de los identificativos de estos eventos son intervenidos entre el momento del almacenamiento y el

momento de la visualización.

[0029] Este objetivo se alcanza por un método de almacenamiento de un evento cifrado por una o unas palabras de control (CW) en una unidad de recepción y de descifrado (STB) conectada a una unidad de seguridad (SC), estas palabras de control (CW) y los derechos necesarios estando contenidos en mensajes de control (ECM), caracterizado por que incluye las etapas siguientes:

- almacenar el evento cifrado así como los mensajes de control (ECM) sobre la unidad de almacenamiento,

- transmitir a la unidad de seguridad (SC) los mensajes de control (ECM),

- verificar si los derechos de acceso a este evento están contenidos en la unidad de seguridad (SC),

- determinar un recibo (Q) sobre todo o parte del mensaje de control (ECM) gracias a una clave secreta (K) contenida en la unidad de seguridad (SC) y propia de cada unidad de seguridad,

- almacenar este recibo (Q) sobre la unidad de almacenamiento.

[0030] Según una primera variante de la invención, este recibo se constituye por una firma sobre todo o parte del mensaje de control y constituye un super derecho que permitirá en el momento de la utilización subsiguiente del evento, verificar prioritariamente este recibo antes de verificar los derechos usuales en la unidad de seguridad. La presencia de este recibo, una vez reconocida para un mensaje de control dado, permite ignorar las condiciones de acceso.

[0031] Según una segunda variante de la invención, en el momento de la generación del recibo, además de la firma, una nueva parte es añadida que describe cómo tratar este mensaje de control cuando éste sea presentado a la unidad de seguridad. Esta condición puede ser ignorar todas las condiciones enunciadas en este mensaje (volviendo a la solución precedente) o enunciar otras condiciones tales como disponer de un derecho de reproducción o definir una ventana en tiempo para autorizar tal reproducción.

[0032] Para determinar la firma, se tomará preferiblemente una parte que es invariada para todo el evento. De hecho, el mensaje ECM incluye esquemáticamente dos partes:

a. la palabra de control para la descifrado (o las palabras par e impar)

b. el derecho necesario para devolver esta palabra de control.

[0033] Este recibo permite marcar un mensaje de control y por lo tanto añadir otras informaciones destinadas al tratamiento en modo reproducción. El objetivo es por lo tanto identificar un mensaje de control de una manera indudable. En la práctica, se constata que la parte b, es decir el derecho necesario, cambia menos frecuentemente que la palabra de control. Por esta razón se elegirá preferiblemente esta parte para calcular la firma. Sin embargo, no se excluye de determinar la firma sobre la palabra de control, o el conjunto de las dos partes.

[0034] Para el cálculo de esta firma, se determina una imagen única de la parte considerada por una función unidireccional y sin colisión sobre estos datos. Se admite que no existe un conjunto de datos diferente que dé el mismo resultado que esta función. Esta imagen H se produce por una función de tipo Hash. El algoritmo utilizado puede ser de tipo SHA-1 o MD5 y esta imagen expresa el conjunto de los datos de una manera única.

[0035] La operación siguiente consiste en cifrar estos datos gracias a una clave de cifrado K.

[0036] Antes la operación de cifrado, por la clave K, es posible añadir un campo de datos CD que describe nuevas condiciones de acceso. El conjunto de estos datos (H y CD) que constituye el recibo es a continuación cifrado por la clave de firma K.

[0037] En el espíritu de la invención, el término recibo significa que se determina un conjunto de datos representativo de las condiciones de acceso (por ejemplo en el caso más sencillo) y único para una unidad de seguridad concernida gracias a la clave de cifrado K. Según una forma de realización, es posible cifrar directamente las condiciones de acceso del mensaje de control ECM por esta clave sin pasar por la operación de Hash. Según otra forma de realización, es posible determinar esta imagen única (función Hash) sobre las condiciones de acceso después de cifrar esta imagen por una primera clave K1, añadir las nuevas condiciones de acceso CD y cifrar todo con la misma clave K1 o una segunda clave K2.

[0038] La invención se comprenderá mejor gracias a la descripción detallada siguiente y que se refiere a los dibujos anexos que se dan a modo de ejemplo en ningún caso limitativo, a saber:

- la figura 1 describe una unidad de usuario STB con unidad de almacenamiento,

- la figura 2, describe el conjunto de los datos almacenados sobre la unidad de almacenamiento,

- la figura 3 describe la estructura de un mensaje de control ECM.

[0039] El descodificador STB ilustrado en la figura 1 recibe los datos en entrada en forma cifrada. Estos datos se memorizan en la unidad de almacenamiento HD y comprenden particularmente el evento considerado EV y los mensajes de control ECM.

[0040] De este modo, según la invención, estos dos conjuntos de datos se acompañan por un nuevo conjunto que se ilustra en la figura 2 por el bloque de recibo Q.

[0041] El tamaño de los diferentes bloques es dado aquí como ejemplo. Se puede sin embargo considerar que el evento EV ocupa la mayor parte, los mensajes de control ECM una pequeña parte y según una forma de realización, un único recibo basta para el conjunto de estos datos.

[0042] De hecho, si esta firma se efectúa sobre la parte de las condiciones de acceso del mensaje de control, no va a variar para todo el evento considerado.

[0043] En la figura 3 se ilustra la estructura de un mensaje de control ECM. Este mensaje contiene, como se ha descrito anteriormente, la palabra de control CW y las condiciones de acceso. Estas condiciones se dividen en dos partes, una parte propia a las condiciones de difusión ACB y una parte propia a las condiciones de reproducción ACR. Este mensaje incluye igualmente una marca tiempo TP.

[0044] Entre estas condiciones, se puede hallar:

- número del canal (o servicios), particularmente útil para el abono,

- el tema del evento (por ej. deporte, noticias, adulto)

- el nivel (prime time, tarde, redifusión)

- un número para compra impulsiva.

[0045] La duplicación de las condiciones abre posibilidades para la gestión del evento en el momento de la reproducción. El recibo Q puede significar que es necesario conformarse sencillamente con las condiciones de reproducción o entonces significar por el contrario ignorar estas condiciones.

[0046] Tomemos el ejemplo de una función de bloqueo geográfico. Esta función permite bloquear la recepción de un evento deportivo por ejemplo en los 30 km alrededor del estadio. Si este bloqueo tiene un sentido en el momento del evento, por el contrario algunos días más tarde, ya no tiene razón de ser.

[0047] En las condiciones de difusión ACB, se hallarán las condiciones del bloqueo por tramo de números de unidad de seguridad o por código postal. Por cuanto concierne a las condiciones de reproducción ACR, se hallará una simple autorización para todos a partir de una cierta fecha (siempre y cuando las otras condiciones tales como abono, se cumplan).

[0048] En el momento de la reproducción, el recibo Q se carga en primer lugar y se descifra por la clave secreta K, para obtener la firma SGN y las nuevas condiciones de acceso CD.

[0049] La firma SGN es a continuación conservada en la memoria de la unidad de seguridad con las nuevas condiciones CD. Cuando se presenta un mensaje de control ECM a la unidad de seguridad, esta determina por la función Hash una imagen única H' sobre la parte de los derechos AC según este ejemplo y compara este valor H' con la firma SGN.

[0050] Si los dos valores son idénticos, la unidad de seguridad aplica las condiciones enunciadas en la parte condiciones CD del recibo. Si esta condición CD significa "acceso libre", esto permite dejar de verificar las condiciones contenidas en el mensaje de control ECM y por lo tanto permite liberarse de todos los cambios estructurales de los canales de difusión.

[0051] Según otro ejemplo de aplicación, la nueva condición CD reenvía a las condiciones de reproducción ACR. En estas condiciones ya no se encuentra referencia a los canales, u otros elementos que podrían variar en el tiempo (condiciones estructurales) sino condiciones sobre el tiempo durante el cual este acceso es acordado o un número de veces. Se sobreentiende en tal caso que las condiciones de acceso ligadas a un abono u otras han sido verificadas en el momento de la formación del recibo.

[0052] El recibo puede ser evolutivo. En cierto caso puede ser interesante almacenar un nuevo recibo más favorable que el antiguo: éste es el caso particularmente en el momento de una compra impulsiva. En tal caso un primer recibo se genera en el momento del almacenamiento sin que el usuario haya comprado este evento.

[0053] Las condiciones contenidas en este recibo reenviarán a las condiciones contenidas en el mensaje de control ECM.

[0054] En el momento en que el usuario decide comprar este evento, un nuevo recibo se genera que abre la vía a una utilización sin reserva de este evento si las condiciones son definidas como tales. Este recibo es entonces transmitido a la unidad de almacenamiento para reemplazar el antiguo.

REIVINDICACIONES

1. Método de almacenamiento de un evento cifrado por una o unas palabras de control (CW) en una unidad de recepción y de descifrado (STB) conectada a una unidad de seguridad (SC), estas palabras de control (CW) y las condiciones de acceso a este evento estando contenidas en mensajes de control (ECM), caracterizado por el hecho de que incluye las etapas que consisten en:

- almacenar el evento cifrado así como el o los mensajes de control (ECM) sobre una unidad de almacenamiento,

- transmitir a la unidad de seguridad (SC), los mensajes de control (ECM),

- verificar si los derechos de acceso a este evento están contenidos en la unidad de seguridad (SC),

- formar un recibo (Q) conteniendo las informaciones destinadas al tratamiento del evento en modo reproducción, este recibo (Q) incluyendo una firma (SGN) sobre todo o parte del mensaje de control (ECM) gracias a una clave secreta (K) contenida en la unidad de seguridad (SC) y propia de cada unidad de seguridad, este recibo siendo tal que en el momento de la utilización subsiguiente del evento, la autenticidad de dicho recibo se verifica prioritariamente antes de verificar los derechos usuales en la unidad de seguridad;

- almacenar este recibo (Q) en la unidad de almacenamiento.

2. Método según la reivindicación 1, caracterizado por el hecho de que la autentificación del recibo incluye las etapas siguientes:

- determinación a partir de todo o parte del mensaje de control de una firma,

- comparación de dicha firma con dicha firma (SGN) del recibo,

- aplicación de las condiciones enunciadas en la parte condición del recibo si la comparación indica que los dos valores son idénticos.

3. Método según la reivindicación 1, caracterizado por el hecho de que la presencia de dicho recibo para un mensaje de control dado permite ignorar las condiciones de acceso.

4. Método según la reivindicación 1, caracterizado por el hecho de que el recibo (Q) incluye además una parte condicional (CD) que describe las nuevas condiciones independientes de la configuración estructural de la difusión del evento.

5. Método según la reivindicación 4, caracterizado por el hecho de que la presencia de dicho recibo para un mensaje de control dado permite utilizar las condiciones de acceso contenidas en dicha parte condicional (CD), en lugar de las condiciones de acceso asociadas a dicho mensaje de control.

6. Método según la reivindicación 1, caracterizado por el hecho de que el recibo (Q) sólo se calcula si los derechos de acceso están presentes en la unidad de seguridad.

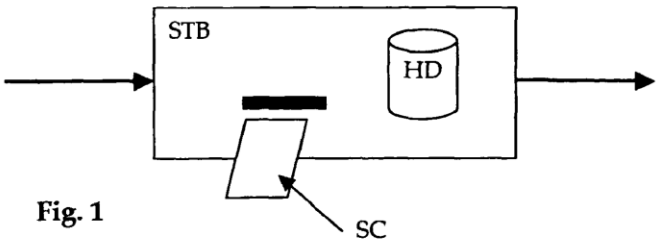

Fig. 1

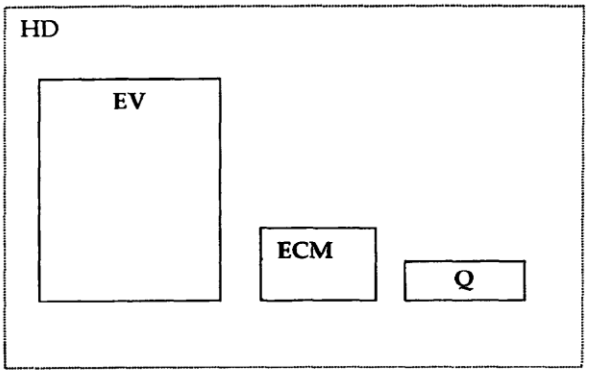

Fig. 2

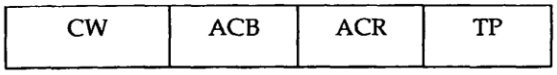

Fig. 3