(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 392 326**

(51) Int. CI.:

H04N 7/16 (2011.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **09783064 .0**

(96) Fecha de presentación: **16.09.2009**

(97) Número de publicación de la solicitud: **2345246**

(97) Fecha de publicación de la solicitud: **20.07.2011**

(54) Título: **Método de aplicación por un centro de gestión de las reglas de acceso a un producto de difusión**

(30) Prioridad:

19.09.2008 EP 08164674
19.09.2008 US 136623 P

(45) Fecha de publicación de la mención BOPI:

07.12.2012

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

07.12.2012

(73) Titular/es:

NAGRAVISION S.A. (100.0%)
Route de Genève 22-24
1033 Cheseaux-sur-Lausanne, CH

(72) Inventor/es:

JUNOD, PASCAL y
KARLOV, ALEXANDRE

(74) Agente/Representante:

TOMAS GIL, Tesifonte Enrique

DESCRIPCIÓN

Método de aplicación por un centro de gestión de las reglas de acceso a un producto de difusión.

Campo de la invención

[0001] Esta invención se refiere al campo de la encriptación de difusión, en particular a la forma de administrar derechos de autorización en un sistema de difusión con un centro de gestión y una pluralidad de dispositivos receptores.

Introducción

[0002] En el modelo de difusión de televisión de pago estándar conocido, como se describe en el "Modelo Funcional de un Sistema de Acceso Condicional EBU", estudio técnico de EBU, invierno de 1995, el producto de televisión de pago que debe ser difundido se encripta y las claves para desencriptar el producto de televisión de pago en el lado receptor se disponen en Mensajes de Control de Derechos (ECM) enviados junto con el producto de televisión de pago codificado. Los ECM se encriptan con una clave de transmisión, que se cambia frecuentemente por razones de seguridad.

[0003] Además de las claves de descodificación, el ECM incluye información sobre los derechos de acceso condicional del producto de televisión de pago en forma de condiciones de acceso que se aplican en el lado receptor.

[0004] Los derechos de acceso condicional del abonado individual (por ejemplo un derecho de suscripción a servicios durante un mes) al igual que las claves de transmisión, se gestionan y se transmiten de manera asincrónica en forma de Mensajes de Gestión de Derechos (EMM). Los EMM se encriptan con claves secretas conocidas sólo por los receptores.

[0005] Para que un dispositivo receptor sea capaz de recibir y desencriptar un producto, el primer paso consiste por lo tanto en recibir y desencriptar los mensajes EMM que incluyen los derechos correspondientes al producto al igual que los mensajes EMM que incluyen las claves de transmisión necesarias para desencriptar los mensajes ECM. Para este fin, el dispositivo receptor comprende una clave única y el EMM se encripta mediante la clave única correspondiente del dispositivo receptor y difundido de modo que sólo este dispositivo particular puede desencriptar el EMM. Para este fin, se pueden utilizar claves simétricas o asimétricas.

Técnica anterior

[0006] Se pueden cargar derechos diferentes en la memoria de los medios de seguridad del dispositivo receptor, estos medios de seguridad se presentan generalmente en forma de tarjeta inteligente, y son aplicados después por los medios de seguridad.

[0007] Estos medios de seguridad puede tener diferentes formas, tales como una tarjeta inteligente, un chip de seguridad, un USB electrónico o un software resistente a manipulaciones en el dispositivo.

[0008] Consideramos que estos medios de seguridad son lo suficientemente seguros para almacenar al menos la clave de transmisión, la única clave perteneciente al dispositivo receptor y el derecho (o derechos) asociado(s) a este dispositivo receptor.

[0009] La función de los medios de seguridad es recibir los mensajes ECM y EMM, desencriptar los ECM usando la clave de transmisión y extraer la clave de acceso (o claves) así como las condiciones de acceso relativas a este producto de televisión de pago. Los medios de seguridad controlan si el derecho que corresponde a las condiciones de acceso contenidas en los ECM está presente en la memoria de los medios de seguridad y en caso positivo, la clave de acceso vuelve al dispositivo receptor para la desencriptación del producto.

[0010] Un ECM puede contener más de una definición de condición de acceso. En este caso, según la política aplicada, los medios de seguridad pueden controlar la presencia de los derechos en su memoria y traer de vuelta la clave de acceso si al menos uno de los derechos está presente (función booleana OR). Según otra política, los medios de seguridad sólo pueden traer de vuelta la clave de acceso si todos los derechos correspondientes al conjunto entero de condiciones de acceso están presentes en la memoria de los medios de seguridad (función booleana AND).

[0011] Las consultas complejas sobre el contenido de la memoria se pueden ejecutar tal como descritas en WO2004052005. La clave de acceso sólo vuelve al dispositivo receptor si las distintas pruebas dan un resultado positivo. No sólo se toma en cuenta los derechos, también se puede usar la fecha de caducidad o la solvencia en la decisión de validez del derecho.

[0012] Los derechos al igual que la clave de transmisión se pueden cargar a través de mensajes EMM en la memoria de los medios de seguridad de varias maneras:

- En la fase de inicialización del dispositivo receptor, mediante una conexión local con el servidor o mediante la recepción de mensajes de inicialización enviados al canal de difusión

- En cualquier momento, por ejemplo cuando se modifican los datos del abonado, durante la suscripción o cancelación de servicios, renovación de derechos, modificación de la clave de servicios (incluyendo la clave de transmisión).

[0013] Con el anuncio de los medios de seguridad realizado sólo por el software, el riesgo de que la seguridad de este software sea comprometida es superior al riesgo con medios de seguridad de hardware específicos.

[0014] Los primitivos de encriptación de difusión tales como el que se describe en "Encriptación Resistente a Colusión con Textos Cifrados Cortos y Claves Privadas" por Dan Boneh, Craig Gentry and Brent Waters son una forma eficaz para transmitir de manera segura un contenido digital mediante un canal de difusión con respecto al ancho de banda del canal, la capacidad de almacenamiento del receptor y la complejidad de encriptación/desencriptación. Consiste en tres algoritmos. Algoritmo de instalación, que inicializa los parámetros del sistema tales como el material de clave de desencriptación para los receptores (objetivos) y una clave de descifrado para el centro de difusión. Un algoritmo encriptado genera un criptograma para un subconjunto autorizado de receptores, de modo que otros receptores al exterior del subconjunto autorizado son incapaces de desencriptar el criptograma. Desencriptar un algoritmo correctamente desencripta el criptograma siempre que el receptor tenga la clave de desencriptación y se encuentre en el subconjunto autorizado.

[0015] El documento US20040168063 divulga un método para controlar el acceso a contenidos basado en una combinación de derechos y claves. Una única clave secreta se almacena en un módulo de conexión y se usa para descifrar un mensaje que contiene otra clave, por ejemplo una clave de producto, para acceder al contenido. El módulo de conexión recibe la clave de acceso al contenido al que tiene permiso de acceder. Esta clave de acceso es encriptada directa o indirectamente por la clave secreta, de modo que sólo el receptor previsto puede tener acceso a ésta. El contenido es accesible por el módulo de conexión en caso de recibir la clave de acceso correcta y basada en el criterio de acceso contenido en los mensajes que acompañan el contenido.

Problema que solucionar

[0016] Teniendo en cuenta una situación en la que la central desea difundir un contenido especial al conjunto autorizado de receptores que cumplen ciertos criterios o características (o carecen de éstos). Esta característica puede ser por ejemplo la suscripción a un paquete de servicios, la cantidad de dinero restante en la tarjeta inteligente, el código postal del receptor (u otra información geográfica), las propiedades del conjunto de chips o cualquier otra información de cliente o relacionada con el dispositivo.

[0017] El beneficio de la presente invención es dirigir de manera eficiente este asunto mediante el uso de dos casos de primitivos de encriptación de difusión en paralelo.

[0018] A diferencia del método descrito en el documento WO2004052005 que tiene una funcionalidad comparativa, la presente invención permite realizar una aplicación adecuada en el centro de difusión (es decir cabecera). Éste tiene una ventaja sobre el método precedente que respeta los derechos en el módulo de seguridad (SC) ya que la seguridad en el caso anterior se basaba en la dificultad de aplicar una ingeniería inversa (pausa) a un módulo de seguridad, mientras que en nuestro caso la seguridad se basa en un problema matemático difícil. También, a diferencia de la descripción del documento WO2004052005, la presente invención puede manejar condiciones y normas de acceso complejas sin ningún impacto para la seguridad del sistema.

Breve descripción de la invención

[0019] El propósito de esta invención es proponer una forma de confiar menos en los medios de seguridad del módulo de seguridad del receptor (SC), por un lado para respetar las condiciones de acceso definidas en los mensajes clave, y por otro lado para manejar condiciones de acceso complejas basadas en la característica y propiedades del dispositivo receptor o del usuario de tal dispositivo.

[0020] Por lo que se propone un método de aplicación por un centro de control de las reglas de acceso a un producto de difusión recibido por receptores, el acceso a dicho producto siendo provisto por una clave de producto, donde dicho centro de control gestiona una pluralidad de paquetes de suscripción para los que al menos un paquete de suscripción permite el acceso al producto, el método comprendiendo las siguientes etapas principales que consisten en:

- definir para cada paquete de suscripción al menos un material de clave positiva y un material de clave negativa,

- para un receptor suscrito a lo menos un paquete de suscripción, cargar el material de clave positiva de dicho paquete de suscripción y el material de clave negativa de los paquetes de suscripción para los cuales no se realizó ninguna suscripción.

[0021] En caso de que algún producto sea accesible por al menos un primer paquete de suscripción y no accesible para al menos un segundo paquete de suscripción:

- preparar un mensaje de autorización para permitir el acceso al producto, la clave de producto o datos que permiten recuperar la clave de producto usada para producir un criptograma, dicho criptograma siendo encriptado por ambas clave de acceso de material de clave positiva del primer paquete de suscripción y material de clave negativa del segundo paquete de suscripción de modo que el criptograma que permite recuperar la clave del producto sólo es accesible cuando el material de clave positiva del primer paquete de suscripción y el material de clave negativa del segundo paquete de suscripción están presentes en el receptor.

[0022] La particularidad del presente método consiste en definir dos materiales de clave para un paquete de suscripción. Una de estas claves (material de clave positiva) se carga cuando se autoriza al receptor al paquete de suscripción y la otra (material de clave negativa) se carga en un receptor que no tiene acceso a dicho paquete de suscripción.

[0023] El centro de control tiene como primer objetivo un atributo (por ejemplo un conjunto de servicios o paquete de suscripción) y realiza una lista de los posibles atributos y determina para cada atributo un material de clave. Por material de clave, se hace referencia a al menos una clave asociada a este atributo y opcionalmente a una definición adecuada.

[0024] Esta invención se basa en el hecho de que para un dispositivo receptor particular autorizado a recibir un primer paquete de suscripción y no un segundo paquete de suscripción, dicho dispositivo receptor recibe el material de clave positiva del primer paquete de suscripción y el material de clave negativa del segundo paquete de suscripción.

[0025] Gracias a este material de clave, los mensajes de clave pueden incluir consultas complejas tales como permitir el acceso a la clave de producto sólo cuando el dispositivo receptor está autorizado a acceder al primer paquete de suscripción y no al segundo paquete de suscripción.

[0026] La clave de acceso o clave de producto se puede utilizar para acceder directamente al producto o acceder indirectamente al producto, es decir, usando otras claves o algoritmos en el módulo de seguridad. Esta clave de acceso se puede combinar con otras claves en el mismo mensaje o en otros mensajes de control de derecho de acceso tales como los que se describen en EP1252768, la clave de acceso en este caso tiene el papel de una clave maestra.

[0027] En una forma de realización alternativa, la clave de acceso es la denominada clave de transmisión que se usa para encriptar (o desencriptar) los mensajes que contienen las palabras de control y las condiciones de acceso.

Breve descripción del dibujo

[0028] La invención se explicará con la ayuda del la figura anexa en la que se ilustra un dibujo general del entorno de difusión.

Descripción detallada de la invención

[0029] Durante la inicialización de un nuevo abonado, el módulo de seguridad de su receptor recibe mensajes con el material de clave dedicado a este usuario.

[0030] Tomemos el ejemplo en el que el centro de gestión controla cuatro paquetes de suscripción, cada paquete contiene al menos un servicio audio/video y puede comprender una pluralidad de servicios. En el caso de que este usuario se haya suscrito a un primer paquete de suscripción, el material de clave positiva del primer paquete de suscripción se envía al receptor para el almacenamiento dentro de su módulo de seguridad. El centro de gestión enviará también el material de clave negativa de los otros paquetes de suscripción a los cuales el abonado no tiene acceso.

[0031] Gracias a esta estructura, ahora es posible definir las condiciones de acceso a un producto de difusión específico usando el material de claves positiva y negativa. Según un ejemplo donde el producto es accesible a un

abonado suscrito al primer paquete y no al segundo paquete, la clave de producto, es decir, la clave para desencriptar el producto es así encriptada por la clave positiva del primer paquete de suscripción y de nuevo por la clave negativa del segundo paquete de suscripción. Un mensaje se forma con esta doble clave encriptada de producto y se envía a los abonados. Nuestro abonado específico con acceso al primer paquete y no al segundo paquete puede después desencriptar este doble clave encriptada de producto. En el caso de que otro abonado tenga acceso al primer y al segundo paquete, dicho abonado no poseerá la clave negativa del segundo paquete de suscripción y será incapaz de desencriptar la clave del producto.

[0032] Las condiciones de acceso al producto son por lo tanto aplicadas por el centro de gestión y no dependen de la verificación realizada por el abonado.

[0033] La orden de encriptación, es decir que se puede invertir la clave positiva y la clave negativa sin consecuencia. La clave negativa se puede usar primero y la clave positiva se puede usar posteriormente.

[0034] En el caso de que la condición de acceso tenga una influencia sobre un tercer paquete de suscripción, la clave de producto también puede ser encriptada por la clave negativa o clave positiva del tercer paquete de suscripción, dependiendo del hecho de que la condición debe o no debe tener acceso al tercer paquete de suscripción.

[0035] Según una forma de realización de la invención, la clave de producto se encripta inicialmente mediante una clave de sesión. Esto permite tratar las claves positiva y negativa de una forma más flexible. En caso de que las claves positiva y negativa sean claves asimétricas, el tamaño del material encriptado por una clave asimétrica se define por el algoritmo asimétrico. Esto tendrá una influencia sólo sobre el tamaño de la clave de sesión y dejará libre el tamaño de la clave de producto. Una clave de producto de 96 bits se puede usar y encriptar mediante una clave de sesión de 128 bits. La clave de sesión se encripta después en función de la condición de acceso y no de la clave de producto como se ha descrito anteriormente. El mensaje enviado a la unidad del abonado contiene la clave de producto encriptada por la clave de sesión, y la clave de sesión encriptada por las claves positiva o negativa según las condiciones de acceso a los paquetes de suscripción.

[0036] Como un abonado puede cambiar sus suscripciones, según una forma de realización de la invención, los materiales de claves positiva y negativa se renuevan regularmente, por ejemplo cada mes. De modo que un abonado no tiene interés en mantener la clave negativa de un paquete de suscripción determinado cuando se suscribe a este paquete. El centro de gestión enviará a este abonado la nueva clave positiva del mes siguiente para los paquetes de suscripción a los que tiene derecho, y la nueva clave negativa del mes siguiente para los paquetes de suscripción a los que no tiene derecho. Por lo que el hecho de conservar en los medios de almacenamiento de la unidad del abonado los elementos del mes precedente no le permite eludir las condiciones de acceso basadas en una combinación de claves positiva y negativa.

Explicación de la figura

[0037] En la Figura 1, el centro de gestión MC almacena en su base de datos DB una copia de los materiales de claves enviados a los dispositivos receptores RD1, RD2, RD3. Según nuestro ejemplo, se han definido dos paquetes de suscripción B1, B2, el primero se relaciona con el material de clave positiva K1 y el material de clave negativa K1', el segundo se relaciona con el material de clave positiva K2 y el material de clave negativa K2'.

[0038] El dispositivo receptor RD1 que tiene derecho a acceder al paquete de suscripción B1 ha recibido el material de clave K1. Debido al hecho de que este dispositivo receptor RD1 no tiene derecho a acceder al paquete de suscripción B2, el material de clave K2 también se envió a este último.

[0039] Como el dispositivo receptor RD2 tiene derecho a acceder al paquete de suscripción B1 y B2, ambos materiales de clave K1 y K2 se enviaron a este dispositivo.

[0040] Como el dispositivo receptor RD2 tiene derecho a acceder al paquete de suscripción B2, el material de clave K2 se envió a este último. Debido al hecho de que este dispositivo receptor RD3 no tiene derecho a acceder al paquete de suscripción B1, el material de clave K1 también se envió a este último.

[0041] Cuando el centro de gestión MC necesita transmitir una clave de acceso sólo a los dispositivos receptores autorizados a acceder al segundo paquete de suscripción B2 y no autorizados a acceder al primer paquete de suscripción B1, el criptograma CY enviado a los dispositivos receptores RD contendrá la clave de acceso combinada con el material de clave negativa K1' y el material de clave positiva K2.

[0042] En el mensaje de autorización conteniendo el criptograma, otro campo dentro del mensaje contiene un descriptor de las claves que se debe usar para la desencriptación. Éste puede tener la forma de dos mapas de bits, donde cada bit activo define un paquete de suscripción, y un mapa de bits para las claves positivas y el otro para las

claves negativas. Según la implementación de la invención, se podría decidir que las claves positivas se usan primero para desencriptar el criptograma y después las claves negativas.

[0043] La clave de producto puede autorizar un único producto de difusión, por ejemplo una película o puede autorizar un servicio para un día o un mes.

[0044] El paquete de suscripción se puede referir a una pluralidad de servicios o a un único servicio. La invención permite así definir la regla de acceso de este producto mediante combinación del acceso al canal 3 (primer paquete de suscripción) y no al canal 6 (segundo paquete de suscripción).

REIVINDICACIONES

1. Método de aplicación por un centro de gestión de las reglas de acceso a un producto de difusión recibido por receptores, el acceso a dicho producto siendo dependiente de una clave de producto, dicho centro de gestión gestiona una pluralidad de paquetes de suscripción para la cual al menos un paquete de suscripción permite el acceso al producto, el método comprendiendo los etapas iniciales que consisten en:

   - definir al menos un material de clave positiva para cada paquete de suscripción, el material de clave positiva comprendiendo al menos una clave positiva y siendo destinado a receptores suscritos al paquete de suscripción,

   - para un receptor con acceso a al menos un paquete de suscripción, cargar el material de clave positiva de dicho paquete de suscripción, **caracterizado por el hecho de que** comprende además las etapas que consisten en:

   - definir para cada paquete de suscripción al menos un material de clave negativa, el material de clave negativa con al menos una clave negativa destinada a los receptores no suscritos al paquete de suscripción,

   - y para dicho receptor, cargar el material de clave negativa de los paquetes de suscripción para los que no se ha hecho ninguna suscripción,
   en caso de que dicho producto sea accesible para al menos un primer paquete de suscripción e inaccesible para al menos un segundo paquete de suscripción:

   - preparar un mensaje de autorización para dar acceso al producto, la clave de producto o de datos que permiten recuperar la clave de producto siendo utilizada para producir un criptograma, dicho criptograma siendo encriptado por la clave positiva del primer paquete de suscripción y la clave negativa del segundo paquete de suscripción de modo que el criptograma que permite recuperar la clave de producto sólo es accesible cuando el material de clave positiva del primer paquete de suscripción y el material de clave negativa del segundo paquete de suscripción están presentes en el receptor.

2. Método según la reivindicación 1, en el que el criptograma es la clave de producto.

3. Método según la reivindicación 1, en el que el criptograma es una clave de sesión, la clave de producto siendo encriptada por la clave de sesión, este método comprendiendo la etapa de adición de la clave de producto encriptada en el mensaje de autorización.

4. Método según cualquiera de las reivindicaciones 1 a 3, en el que el criptograma se genera por encriptación secuencial del criptograma por al menos una clave negativa y al menos una clave positiva.

5. Método según cualquiera de las reivindicaciones 1 a 4 en el que el mensaje de autorización comprende una información de identificación que describe los paquetes de suscripción usados para la encriptación.

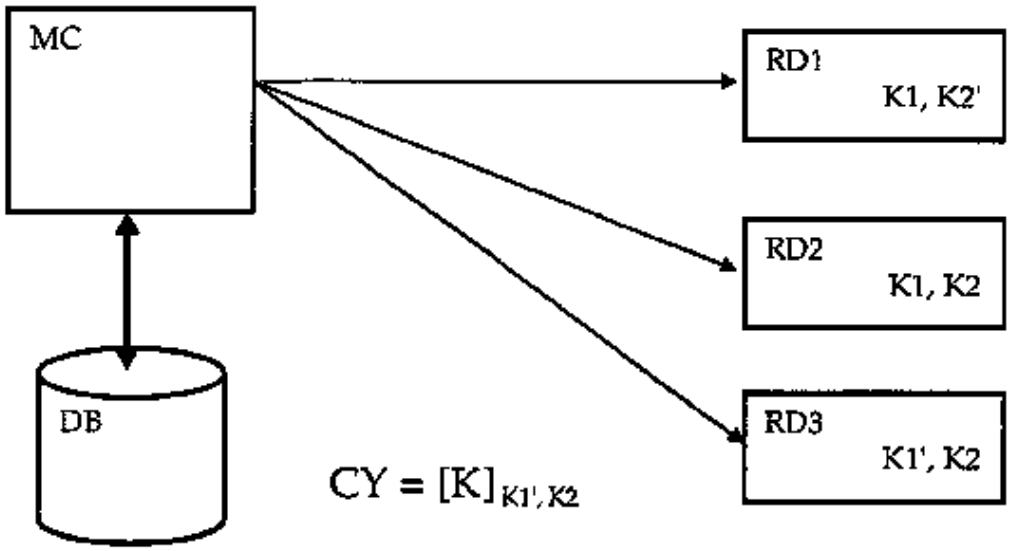

Fig. 1