(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 340 990**

(51) Int. Cl.:
H04N 5/00 (2006.01)
H04N 7/16 (2006.01)
H04N 7/167 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **03013604 .8**
(96) Fecha de presentación : **16.06.2003**
(97) Número de publicación de la solicitud: **1377035**
(97) Fecha de publicación de la solicitud: **02.01.2004**

(54) Título: **Método de actualización de las claves de seguridad en un descodificador de televisión.**

(30) Prioridad: **28.06.2002 CH 1126/02**

(45) Fecha de publicación de la mención BOPI:
14.06.2010

(45) Fecha de la publicación del folleto de la patente:
14.06.2010

(73) Titular/es: **Nagravision S.A.**
route de Geneve 22-24
1033 Cheseaux-sur-Lausanne, CH

(72) Inventor/es: **Brique, Olivier;**
Gogniat, Christophe y
Kudelski, Henri

(74) Agente: **Tomás Gil, Tesifonte Enrique**

DESCRIPCIÓN

Método de actualización de las claves de seguridad en un descodificador de televisión.

La presente invención se refiere al ámbito de los receptores de televisión de pago, en particular a la seguridad de los enlaces entre un receptor y su módulo de seguridad.

En un sistema de televisión digital de pago, el flujo digital transmitido hacia estos receptores es encriptado para poder controlar su utilización y definir las condiciones para tal utilización. Este encriptado se realiza gracias a unas palabras de control (Control Words) que se cambian en intervalos regulares (normalmente entre 5 y 30 segundos) con el fin de disuadir cualquier ataque destinado a recuperar tal palabra de control.

Para que el receptor pueda desencriptar el flujo encriptado por esas palabras de control, estas últimas son enviadas a dicho receptor independientemente del flujo en mensajes de control (ECM) encriptados por una clave propia al sistema de transmisión entre el centro de gestión (CAS) y el módulo de seguridad de la unidad de usuario. En efecto, las operaciones de seguridad se efectúan en una unidad de seguridad (SC) que tiene generalmente la forma de una tarjeta chip, considerada inviolable. Esta unidad puede ser de tipo móvil o integrada directamente en el receptor.

Las palabras de control son devueltas después al descodificador para poder desencriptar el flujo encriptado.

Para impedir que estas palabras de control sean interceptadas durante sus transmisiones hacia el descodificador, este enlace se protege sea por claves de sesión como descrito en el documento WO97/38530 o bien por una clave de comparación como descrito en el documento WO99/57901.

En el segundo documento citado, una clave secreta se incluye en el receptor que se empareja con el módulo de seguridad, el cual se conecta durante una fase de inicialización. Esta clave puede ser de tipo simétrico o asimétrico. Los dos dispositivos son por lo tanto inseparables desde el punto de vista operativo.

Sin embargo, puede ser útil que esta seguridad evolucione, por ejemplo para reemplazar una clave de cierta tecnología (longitud de clave por ejemplo) por otra tecnología.

Esta operación incluye en sí un riesgo importante de fraude ya que consiste en instalar a distancia nuevos medios de seguridad. Se sabe que unos receptores están en manos de personas al acecho de todas las informaciones que les permita quebrantar la seguridad dispuesta.

Por esta razón, la presente invención se propone la evolución de una primera seguridad basada en una primera clave hacia una segunda seguridad basada en una segunda clave, esta operación siendo efectuada en un medio no protegido por una transmisión conocida abierta, garantizando el mismo nivel de seguridad que si esta operación se efectuara localmente en un lugar propio al gestor del sistema.

Este objetivo se alcanza por un método tal como definido en la reivindicación 1.

De esta manera, un mensaje interceptado y desencriptado por la clave pública común transmitida previamente no permite recuperar la nueva clave pública ya que sólo la primera clave personal del descodificador es capaz de descodificar el mensaje.

De este modo, este método garantiza el hecho de que esta nueva clave se instale en el sitio donde la primera clave está almacenada. Si un descodificador no posee esta clave, no se instalará ninguna clave nueva.

Según un modo de funcionamiento, esta primera clave es la clave que sirve al emparejamiento con la unidad de seguridad. Como indicado más arriba, ésta puede ser de tipo simétrico o de tipo asimétrico. En el segundo caso, se colocará la clave privada en la unidad de seguridad y la clave pública en el descodificador.

De la misma manera, durante la preparación del mensaje cifrado, la nueva clave asimétrica será cifrada por la clave privada correspondiente a la primera clave pública de dicho descodificador.

Una verificación suplementaria es aplicada por el programa de actualización, verificación basada en el número único del descodificador. El mensaje contiene también el número único UA del descodificador. Este número se desencripta por la clave pública común. De este modo, antes de utilizar la primera clave del descodificador, el programa verifica si el número único es conforme a lo que estaba previsto.

El descodificador posee así dos claves personales, a saber la primera clave y la nueva clave pública. Estas dos claves van a ser utilizadas en el mecanismo de emparejamiento con la unidad de seguridad.

Con el fin de garantizar el buen funcionamiento del conjunto, la unidad de seguridad deberá recibir también una nueva clave privada que corresponde a la nueva clave pública recibida por el descodificador. Para ello, dispone de medios de seguridad para la transmisión protegida de esta clave que después se carga en la memoria no volátil de esta unidad. Se puede añadir un nivel de seguridad adicional a la encriptación por una clave de sistema, mediante el

encriptado de esta clave privada por la primera clave. De este modo, cada mensaje se vuelve único y relacionado con la condición de conocer la primera clave.

Esta estructura permite que pueda evolucionar una seguridad que utiliza una clave de seguridad, hacia una seguridad que utiliza dos claves (o más) sin rotura en el mecanismo de actualización.

Durante este proceso, se recomienda verificar si la clave recibida es la correcta y por eso, se añade a la nueva clave asimétrica, un identificador constante conocido del programa de actualización. De este modo, este programa va a verificar que la clave es valida antes de introducirlo en su memoria.

En la práctica, la unidad de seguridad del descodificador es la que va a recibir el mensaje encriptado y transmitirlo al descodificador. Cuando esta unidad se filtra con el descodificador, el mensaje transmitido de este modo se encripta por la primera clave que es la clave de emparejamiento.

Referencias citadas en la descripción

Esta lista de referencias citada por el solicitante ha sido recopilada exclusivamente para la información del lector. No forma parte del documento de patente europea. La misma ha sido confeccionada con la mayor diligencia; la OEP sin embargo no asume responsabilidad alguna por eventuales errores u omisiones.

Documentos de patente citados en la descripción

-WO 9738530 A [0005] - WO 9957901 A [0005]

REIVINDICACIONES

1. Método de actualización de la seguridad aplicada al enlace entre un descodificador y su unidad de seguridad comprendiendo una primera clave filtrada, dicho descodificador comprendiendo un número único y siendo conectado a un centro de gestión, este método comprendiendo las etapas siguientes:

- transmisión desde el centro de gestión hacia los descodificadores referidos, de una clave pública común y de un programa de actualización,
- preparación para el centro de gestión y para cada descodificador, de un mensaje cifrado, este mensaje conteniendo el número único del descodificador así como una nueva clave asimétrica pública cifrada por la primera clave de dicho descodificador y por la clave privada común,
- ejecución en el descodificador del programa de actualización y verificación del número único del descodificador con el número recibido en el mensaje y extracción de la nueva clave asimétrica pública del mensaje gracias a la clave pública común y a su primera clave,
- almacenamiento de esta nueva clave asimétrica pública en el descodificador,
- transmisión del centro de gestión hacia la unidad de seguridad de la nueva clave asimétrica privada por un mensaje protegido,
- almacenamiento de esta nueva clave asimétrica privada en la unidad de seguridad.

2. Método según la reivindicación 1, **caracterizado** por el hecho de que la primera clave es de tipo simétrico.

3. Método según la reivindicación 1, **caracterizado** por el hecho de que la primera clave es de tipo asimétrico, la nueva clave asimétrica pública es cifrada por la primera clave privada correspondiente a la primera clave pública de dicho descodificador.