(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 517 866**

(51) Int. CI.:

H04N 7/16 (2011.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **02.11.2006 E 06829929 (6)**

(97) Fecha y número de publicación de la concesión europea: **27.08.2014 EP 1946552**

(54) Título: **Método de protección de datos intercambiados entre un dispositivo de tratamiento multimedia y un módulo de seguridad**

(30) Prioridad:

03.11.2005 EP 05110316

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
04.11.2014

(73) Titular/es:

NAGRAVISION SA (100.0%)
22, ROUTE DE GENÈVE
1033 CHESEAUX-SUR-LAUSANNE, CH

(72) Inventor/es:

MOREILLON, GUY;
FISCHER, NICOLAS;
KEYCHENKO, NIKOLAI y
WENGER, JOEL

(74) Agente/Representante:

TOMAS GIL, Tesifonte Enrique

DESCRIPCIÓN

Método de protección de datos intercambiados entre un dispositivo de tratamiento multimedia y un módulo de seguridad

Introducción

[0001] La presente invención se refiere al dominio de los descodificadores para televisión de pago, en particular los descodificadores que disponen de un módulo de seguridad para asegurar las funciones de autorización.

Estado de la técnica

[0002] Un descodificador de televisión de pago comprende esquemáticamente un receptor capaz de recibir y dar forma a las señales de diversas fuentes tales como satélite, cable, red IP; una unidad de filtrado capaz de extraer uno o varios flujos de datos entre la multitud de los flujos posibles; una unidad central encargada de gestionar el conjunto y de asegurar la interfaz usuario; un modulador para transmitir las señales claras hacia un órgano de visualización; así como un módulo de descifrado y de descompresión que recibe el flujo de datos encriptados que provienen de la unidad de filtrado y transmite los datos en claro al demodulador, este módulo que tiene la tarea de descifrar el flujo de datos y de descomprimir dichos datos según un formato estándar como DVB.

[0003] Cabe señalar que físicamente, el módulo de descifrado y de descompresión se coloca sobre el mismo soporte que el modulador de tal manera que los datos en claro no estén accesibles después su descifrado. Un tal descodificador se conecta a una unidad de seguridad que puede tomar varias formas tales como una tarjeta inteligente, una tarjeta tarjeta SIM, un módulo electrónico de cualquier forma cuyo enlace con el descodificador puede ser con o sin contactos.

[0004] Un descodificador puede adoptar numerosas formas tales como el bien conocido aparato puesto a lado del televisor pero también puede estar en la forma de dispositivos portátiles, tales como Palm, teléfono de 3ª generación o iPod™.

[0005] Para asegurar la seguridad de los intercambios entre el módulo de seguridad y el descodificador, los datos transmitidos por el módulo de seguridad se encriptan por una clave propia en cada descodificador. Tal solución se describe en el documento WO99/57901A1. Las claves necesarias para el descifrado de un contenido audio o video son por lo tanto extraídas de mensajes de seguridad que solo puede descodificar este módulo después de la verificación de los derechos.

[0006] Estas claves o contraseñas de control se encriptan con una clave propia al conjunto módulo de seguridad / descodificador y se transmiten al descodificador.

[0007] Con el fin de reforzar la seguridad particularmente en el descodificador, las contraseñas de control se desencriptan en el módulo de descifrado. Cada uno de estos módulos dispone de una clave propia que se comunica al módulo de seguridad por unos medios seguros administrados por un centro de gestión. Un tal ejemplo es igualmente ilustrado en el documento WO2004/010698 en el cual una clave de descifrado está directamente localizada en el módulo de descifrado del flujo, esta clave permitiendo descodificar las claves enviadas por un módulo de seguridad.

[0008] Los procedimientos de establecimiento de una clave de codificación del canal entre el descodificador y el módulo de seguridad se basan en el conocimiento de un secreto común (ver documento WO03107585 o US2004/0088558). Así, si un descodificador debe poder recibir los datos de varios módulos de seguridad, cada módulo debe disponer del secreto inicial para crear este canal protegido.

[0009] El documento XP040400335 de la SCTE (Society of Cable Telecommunications Engineers, Inc), titulado « Copy Protection for POD Module Interface » SCTE DVS/213,1 de junio de 1999, describe un mecanismo de protección de un contenido cambiado entre un módulo de seguridad y un dispositivo huésped. Para ello, el módulo descifra un contenido (proveniente por ejemplo de diversos servicios) y vuelve a codificar este contenido con ayuda de una clave compartida por el huésped y por el módulo. El módulo y el huésped posee cada uno una clave privada así como la clave pública correspondiente. Ellos comunican mutuamente su clave pública y utilizan cada uno la clave pública del otro para poder formar la clave compartida a partir de su propia clave privada. Así la clave compartida se determina a partir de dos claves, a saber una clave pública y una clave privada.

[0010] El documento WO 99/18729 describe un método y un dispositivo para la transmisión y la recepción de datos cifrados en el cual el flujo de palabras de control descifrado es reencriptado antes de ser devuelto al descodificador por el módulo de seguridad. Esta reencriptación es efectuada utilizando una clave compartida que dependa de un valor N asociado a la identificación del descodificador. Este valor se utiliza para diversificar la clave compartida, conocida de antemano por el descodificador y por el módulo de seguridad. El descodificador descifrará el flujo con ayuda de esta clave y de este valor. La obtención de la clave compartida resulta de una transmisión previa al final de la cual es almacenada de forma estable en la memoria ROM del descodificador.

[0011] Para establecer un canal protegido entre un descodificador y un módulo de seguridad, el documento US

2004/088558 sugiere el uso de una sucesión de claves jerarquizadas. Para ello describe un dispositivo decodificador utilizando una clave única que es propia así como un circuito lógico que permite generar una sucesión de tres valores interdependientes de los cuales la primera, función de la clave única y de un valor aleatorio, sirve de clave de cifrado de un contenido y cuyo tercer valor, deducido del segundo valor, sirve de clave de descifrado del contenido cifrado. Como alternativa, una clave de confrontación que implica el primer valor se puede utilizar para la obtención del segundo valor.

[0012] El documento US 2005/0111666 propone un método que apunta a evitar el recurso sistemático de una misma clave de seguridad en el cifrado, por un algoritmo inicial, de las comunicaciones entre dos aparatos. Para ello, se propone modificar esta clave de seguridad sobre la base de un identificador de algoritmo y de una clave inicialmente compartida en el momento de un procedimiento de acuerdo de clave entre estos dos aparatos.

[0013] La necesidad de interactividad siendo creciente, se vuelve necesario abrir el uso de un mismo descodificador a varios operadores o varias entidades, una entidad que constituye un grupo de descodificadores ligados por un mismo denominador común (regional, tipo de contrato, versión del material etc.).. Esto fuerza evidentemente la diseminación de la clave secreta del módulo de descifrado entre las diferentes entidades. Si una de las entidades es el objeto de una fuga, imaginemos el problema que eso crea no sólo para esta entidad, sino para todas las entidades.

Breve descripción de la invención

[0014] El objetivo de la presente invención es proponer un método de creación de un canal protegido y autenticado entre un dispositivo de tratamiento multimedia y un módulo de seguridad que se puede compartir entre varias entidades, sin que los datos transmitidos a una entidad comprometan a otras entidades.

[0015] Este objetivo se alcanza por un método conforme al enunciado de la reivindicación 1.

[0016] Así, una clave de seguridad diferente se genera para cada grupo de módulo de seguridad que permite el diálogo con el mismo dispositivo de tratamiento multimedia.

[0017] Esto tiene la ventaja de que ninguna entidad dispone de la clave personal del dispositivo de tratamiento multimedia pudiendo cambiar los datos protegidos con dicho módulo de seguridad.

[0018] La función de dirección única puede ser de diferentes tipos tales como por ejemplo una función de comprobación aleatoria (SHA, MD2, MD5, HMAC), una función de comprobación aleatoria con clave (HMAC) o una función de codificación, el identificador de operador estando encriptado por la clave personal del dispositivo de tratamiento multimedia.

Breve descripción de la figura

[0019] La invención se comprenderá mejor gracias a la descripción detallada siguiente y que se refiere al dibujo anexo que se da a modo de ejemplo en ningún caso limitativo, y representa un dispositivo de tratamiento multimedia que se puede conectar a dos módulos de seguridad.

Descripción detallada de la invención

[0020] La descripción detallada se refiere a la figura 1. El marco de esta invención es la posibilidad de proteger un canal de comunicación asegurando la gestión por un centro de gestión. Este centro de gestión dispone de la lista de las claves personales relativas a los dispositivos de tratamiento multimedia. En la continuación de la exposición, hablaremos de un descodificador STB como se ilustra en la figura 1.

[0021] Este descodificador STB comprende un módulo de descifrado y de descompresión DD que recibe los datos multimedia en forma encriptada y que los trata con el fin de volverlos utilizables en un órgano de visualización tal como una televisión TV.

[0022] Para efectuar una desencriptación de los datos, es necesario disponer de las claves de desencriptación que se proporcionan por un módulo de seguridad M. El canal entre el módulo de seguridad M y el módulo DD es encriptado por una clave de seguridad con el fin de evitar que una clave de desencriptación pueda ser utilizada por más de un descodificador. Es la manera de generar esta clave que se describe aquí.

[0023] Un centro de gestión se solicita para el establecimiento de los parámetros de seguridad entre una entidad dada y un descodificador. La primera operación es atribuir a esta entidad un identificador CAS_ID que le es propia. La segunda operación es identificar un descodificador y así mismo, conocer su clave personal RK.

[0024] En base a estas dos informaciones, el centro de gestión va a calcular una clave de seguridad VK por una función de dirección única que utiliza estas dos informaciones. La solución más sencilla es una función de comprobación aleatoria (Hash) sobre el bloque formado por el identificador de la entidad y de la clave personal (HMAC). Este resultado constituye la clave de seguridad VK y su conocimiento por el operador no le permite recuperar la clave personal RK.

[0025] Esta clave de seguridad VK es entonces cargada en el módulo de seguridad M, sea al inicio, sea en el momento de una fase de puesta en servicio por el envío de mensajes de gestión por la entidad, a través de los datos multimedia.

[0026] Para que un descodificador pueda generar la clave de seguridad VK, debe conocer el identificador de la entidad CAS_ID. Esta información se puede obtener de varias maneras, por ejemplo por la extracción de datos que están en el flujo de datos multimedia. En caso de que este descodificador se destine a recibir un flujo de datos de una sola fuente, es posible colocar en este flujo la información del identificador de la entidad.

[0027] Según otra forma de realización, es el módulo de seguridad M que va transmitir esta información al módulo de descifrado y de descompresión DD. Es este segundo modo el que ha sido elegido para ilustrar la presente solicitud sin excluir la funcionalidad según el primer modo.

[0028] Cuando un módulo de seguridad desea dialogar con un descodificador STB, por ejemplo el módulo M1, y en particular con su módulo de descifrado y de descompresión DD, este módulo envía su identificador de entidad CAS_ID1 al módulo de descifrado y de descompresión DD. Este último calcula la misma función de dirección única que se efectúa por el centro de gestión y obtiene la clave de seguridad VK1a. Esta clave se utiliza para descodificar los datos recibidos del módulo de seguridad M1. Si este módulo no dispone de esta clave para encriptar las informaciones, los datos obtenidos del lado del módulo de descifrado y de descompresión DD serán incomprensibles. Para evitar todo deterioro del material, es posible añadir una fase de verificación en cuanto que la clave de seguridad se determina por el módulo de descifrado y de descompresión DD. Así, se especifica que el próximo mensaje producido por el módulo de seguridad es un dato de referencia (por ejemplo 01010101B) encriptado por la clave de seguridad VK1a. Si este valor no se recibe por el módulo de descifrado y de descompresión DD, todo tratamiento es interrumpido. En un modo más elaborado, el módulo de descifrado y de descompresión DD genera un número aleatorio N y lo codifica con la clave de seguridad y envía este criptograma al módulo de seguridad. Este último desencripta el criptograma para obtener el número aleatorio N. Aplica una función convenida sobre el número aleatorio (una adición, sustracción, XOR etc.) para obtener N'. El módulo de seguridad codifica N' con la clave de seguridad y envía este criptograma al módulo de descifrado y de descompresión DD. Este último desencripta el criptograma y verifica la relación entre el número aleatorio generado N y el recibido N'. Si la relación es aquella que ha sido convenida, esto significa que las dos partes disponen de la misma clave.

[0029] Según una forma de realización, el identificador de la entidad se puede extender a un identificador de módulo de seguridad. De hecho, el centro de gestión que conoce el descodificador en cuestión y por lo tanto su módulo de descifrado y de descompresión DD y el módulo de seguridad que se destina a interactuar con este descodificador, puede generar una clave de seguridad que sería una función de un identificador de módulo de seguridad y de la clave personal del módulo de descifrado y de descompresión DD. Esta función crea una confrontación entre el módulo de seguridad M1 y el módulo de descifrado y de descompresión DD.

[0030] Según una variante de esta realización, el identificador de módulo de seguridad es formado por dos partes, sea de un identificador de operador o de un identificador propio a este módulo en la clasificación de la entidad.

[0031] Esta manera de codificar el identificador será útil para los modos de realización que implican la verificación del identificador en una lista, solo la parte del identificador relativa a la entidad será verificada por el módulo de descifrado y de descompresión DD.

[0032] Según una variante de realización, el módulo de descifrado y de descompresión DD comprende medios de verificación de la conformidad del módulo de seguridad M que está conectado con el mismo. Con este fin, el módulo de descifrado y de descompresión DD comprende una lista de los identificadores admitidos para la creación de la clave de seguridad tal como se ilustra en la figura 1 por la lista de los CAS_ID. En tal caso se llama positiva porque incluye las CAD_ID válidas o puede ser negativa porque incluye la lista de los CAD_ID prohibidos.

[0033] Existen numerosas maneras de gestionar esta lista y vamos a explicar algunas de estas maneras.

Lista con fusible

[0034] En primer lugar, cada módulo de descifrado y de descompresión DD comprende una lista de por ejemplo 100 identificadores CAD_ID1... ... CAS_ID100. El centro de gestión puede insertar en el flujo de datos multimedia pedidos de desactivación de uno o varios identificadores lo que va tener como consecuencia borrar definitivamente uno o varios identificadores. Esto tendrá como efecto que estos identificadores ya no serán admitidos para crear una clave de seguridad con un módulo de seguridad.

[0035] Estos pedidos de desactivación son preferiblemente encriptados o firmados por una clave que sería común para todos los módulos de descifrado y de descompresión DD.

Lista evolutiva

[0036] El flujo de datos multimedia comprende las informaciones que permiten formar esta lista. En el origen, no se admite ningún identificador (eventualmente un identificador por defecto CAD_ID1) y los pedidos permiten programar los identificadores autorizados o borrar los identificadores revocados. El resultado de estos pedidos se almacena en una memoria no volátil. Al igual que previamente, estos pedidos son preferiblemente encriptados o firmados por una clave común para todos los módulos de descifrado y de descompresión DD.

[0037] Según una forma de realización, el módulo de descifrado y de descompresión DD comprende una memoria volátil que está vacía en el momento de cada conexión. Así, esta memoria se carga con los identificadores recibidos en el flujo de datos multimedia habitual. Esto permite conectar un flujo de datos multimedia a un conjunto de identificadores de entidades dado. Estos identificadores se colocan en una tabla y forman parte del flujo de información SI. Así es posible hacer evolucionar esta tabla durante una misma sesión de difusión y con ella, la lista de las entidades autorizadas. El módulo de descifrado y de descompresión DD memoriza el identificador de la entidad con la cual ha creado una clave de seguridad y cuando la tabla de los identificadores cambia, verifica que el identificador habitual está siempre comprendido en la nueva tabla. En caso contrario, detiene la recepción de los datos transmitidos por este módulo de seguridad y solicita una nueva fase de inicialización de la clave de seguridad.

REIVINDICACIONES

1. Método de protección de datos intercambiados entre un dispositivo de tratamiento multimedia (STB) y un módulo de seguridad (M), el módulo de seguridad (M) siendo administrado por un centro de gestión que dispone de una lista de claves personales (RK) relativas a los dispositivos de tratamiento multimedia, el centro de gestión siendo solicitado para el establecimiento de los parámetros de seguridad entre dicho dispositivo de tratamiento multimedia (STB) y un operador, el dispositivo de tratamiento multimedia (STB) recibiendo un flujo de datos multimedia encriptados y estando encargado de descodificar y convertir estos datos con ayuda de claves de desencriptación proporcionadas por el módulo de seguridad (M) para volverlas legibles, dicho dispositivo de tratamiento multimedia (STB) incluyendo una clave personal (RK), este método incluye las etapas siguientes:
- cálculo, por el centro de gestión, de una clave de seguridad (VK) formada por una operación de dirección única basada en la clave personal (RK) del dispositivo de tratamiento multimedia (STB) y de un identificador (CAS_ID) atribuido por dicho centro de gestión al operador,
- carga de dicha clave de seguridad (VK) en el módulo de seguridad (M), dicho módulo de seguridad conteniendo también el identificador (CAS_ID),
- obtención, por el dispositivo de tratamiento multimedia (STB), del identificador (CAS ID) contenido en dicho módulo de seguridad (M),
- cálculo, por dicho dispositivo de tratamiento multimedia (STB), de dicha clave de seguridad (VK) por una operación de dirección única basada en la clave personal (RK) de dicho dispositivo de tratamiento multimedia (STB) y del identificador (CAS_ID) obtenido por el dispositivo de tratamiento multimedia,
- utilización de la clave de seguridad (VK) para proteger los datos intercambiados entre el dispositivo de tratamiento multimedia (STB) y el módulo de seguridad (M).

2. Método según la reivindicación 1, caracterizado por el hecho de que el módulo de seguridad (M) transmite el identificador (CAS_ID) a dicho dispositivo de tratamiento multimedia (STB).

3. Método según la reivindicación 1, caracterizado por el hecho de que el dispositivo de tratamiento multimedia (STB) obtiene el identificador (CAS_ID) por extracción de dicho identificador (CAS_ID) del flujo de datos recibido.

4. Método según las reivindicaciones 1 a 3, caracterizado por el hecho de que el dispositivo de tratamiento multimedia (STB) comprende un módulo de descifrado y de descompresión (DD) en el cual se inicia la clave personal (RK).

5. Método según la reivindicación 4, caracterizado por el hecho de que comprende una etapa de verificación de la identidad de la clave de seguridad (VK) en el módulo de seguridad (M) y en el módulo de descifrado y de descompresión (DD) por la encriptación con dicha clave de un mensaje que contiene al menos una parte predeterminada por el módulo de seguridad (M), y verificación de esta parte predeterminada después de la desencriptación por el módulo de descifrado y de descompresión (DD).

6. Método según una de las reivindicaciones 1 a 5, caracterizado por el hecho de que la operación de dirección única es una función de tipo hash o hash MAC.

7. Método según una de las reivindicaciones 1 a 5, caracterizada por el hecho de que la operación de dirección única es una función de codificación del identificador (CAS_ID) por la clave personal (RK).

8. Método según una de las reivindicaciones 4 a 7, caracterizado por el hecho de que el módulo de descifrado y de descompresión (DD) comprende una lista de identificadores (CAS_ID1 ...CAS_IDn), este módulo de descifrado y de descompresión (DD) verificando la conformidad del identificador recibido del módulo de seguridad (M) con respecto a esta lista.

9. Método según la reivindicación 8, caracterizado por el hecho de que el dispositivo de tratamiento multimedia (STB) recibe los datos multimedia que incluyen los datos que permiten componer esta lista de identificadores (CAS_ID1...CAS_IDn). ...CAS_IDn)..

10. Método según las reivindicaciones 8 o 9, caracterizado por el hecho de que el módulo de descifrado y de descompresión (DD) comprende una clave para descodificar o verificar la firma de los datos de la lista transmitida.

11. Método según una de las reivindicaciones 8 a 9, caracterizado por el hecho de que la lista de identificadores (CAS_ID1 ...CAS_IDn) es una lista llamada positiva es decir incluyendo los identificadores autorizados en la creación de la clave personal.

12. Método según una de las reivindicaciones 8 a 9, caracterizado por el hecho de que la lista de identificadores (CAS_ID1 ...CAS_IDn) es una lista llamada negativa es decir incluyendo los identificadores prohibidos en la creación de la clave personal.

13. Módulo de descifrado y de descompresión (DD) destinado a ser instalado en un dispositivo de tratamiento multimedia (STB) e incluyendo una unidad central, un módulo de descifrado, un módulo de descompresión, al menos

una clave personal (RK), medios de generación de una clave protegida (VK) calculada a partir de una función de dirección única basada en la clave personal (RK) y en un identificador (CAS_ID) contenido en un módulo de seguridad (M) y recibido por dicho módulo de descifrado y de descompresión (DD), dicho módulo de seguridad (M) estando destinado a ser conectado al dispositivo de tratamiento multimedia (STB) para asegurar las funciones de autorización, caracterizado por el hecho de que está además destinado a recibir de dicho módulo de seguridad (M) datos encriptados por una misma clave de seguridad (VK) calculada por un centro de gestión y cargada en dicho módulo de seguridad (M).

14. Módulo de descifrado y de descompresión (DD) según la reivindicación 13, caracterizado por el hecho que comprende una memoria que contiene una lista de identificadores (CAS_ID1 ...CAS_IDn) y medios de verificación de conformidad con el identificador recibido del módulo de seguridad con respecto a esta lista.

15. Módulo de descifrado y de descompresión (DD) según la reivindicación 13 o 14, caracterizado por el hecho que comprende una clave común y medios para descodificar o verificar la lista de los identificadores (CAS_ID1 ...CAS_IDn) recibidos.

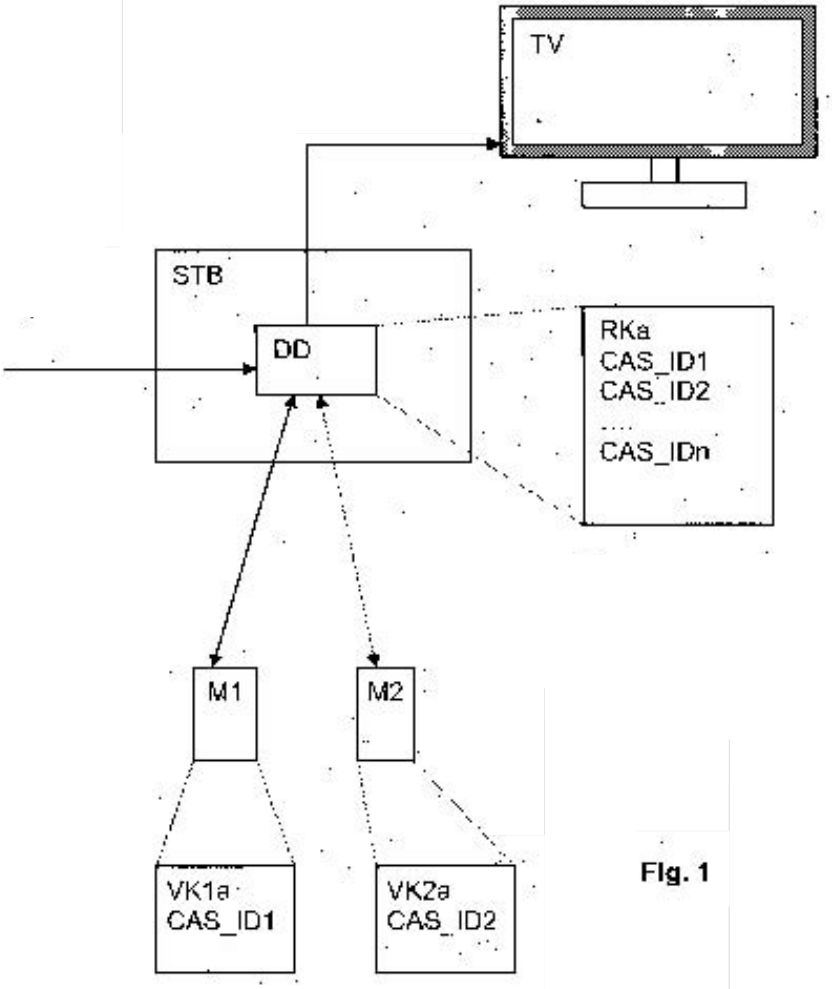
TV
STB
DD
RKa
CAS_ID1
CAS_ID2
....
CAS_IDn
M1
M2
VK1a
CAS_ID1
VK2a
CAS_ID2

Fig. 1