(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 486 251**

(51) Int. CI.:

H04N 21/418 (2011.01)
H04N 21/442 (2011.01)
H04N 21/4623 (2011.01)
H04N 21/472 (2011.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **28.11.2005 E 05810952 (1)**

(97) Fecha y número de publicación de la concesión europea: **07.05.2014 EP 1829370**

(54) Título: **Procedimiento de control de acceso a datos con acceso condicional**

(30) Prioridad:

29.11.2004 EP 04106163

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
18.08.2014

(73) Titular/es:

NAGRAVISION S.A. (100.0%)
ROUTE DE GENÈVE 22-24
1033 CHESEAUX-SUR-LAUSANNE, CH

(72) Inventor/es:

COURTIN, NICOLAS;
BRIQUE, OLIVIER;
COCHARD, JIMMY y
GOGNIAT, CHRISTOPHE

(74) Agente/Representante:

TOMAS GIL, Tesifonte Enrique

DESCRIPCIÓN

Procedimiento de control de acceso a datos con acceso condicional

Campo técnico

[0001] La presente invención se refiere a un procedimiento de control de acceso a datos con acceso condicional en una unidad multimedia que comporta al menos un módulo de seguridad.

[0002] Se refiere también a un módulo de seguridad destinado al acceso a datos con acceso condicional, este módulo de seguridad es en particular un módulo de seguridad desmontable del tipo tarjeta inteligente con un crédito inicial y destinado a ser utilizado en el ámbito de la televisión de pago.

Técnica anterior

[0003] Existe actualmente módulos de seguridad desmontables tales como tarjetas inteligentes con un crédito inicial. Estos módulos de seguridad, denominados tarjetas prepagadas, se utilizan particularmente junto con descodificadores, en el ámbito de la televisión de pago o con acceso condicional. En este contexto, permiten el descifrado de contenidos cifrados.

[0004] De manera bien conocida, en dichos sistemas que utilizan un módulo de seguridad, el contenido se cifra mediante contraseñas de control, luego se envía a las unidades multimedia ligadas a un proveedor de datos o de contenido. Las contraseñas de control se envían a las unidades multimedia, de forma cifrada, en mensajes de control ECM. Estos mensajes de control ECM son transmitidos por el descodificador de la unidad multimedia al módulo de seguridad de esta unidad. Si los derechos de descifrado están presentes, los mensajes de control se descifran para extraer las contraseñas de control. Éstas son devueltas al descodificador, que las utiliza para descifrar el contenido.

[0005] En la práctica, los módulos de seguridad no contienen inicialmente ningún derecho. Éstos se transmiten en el momento de una fase de inicialización que es realizada habitualmente por un técnico en el momento de la instalación de la unidad multimedia. Eso significa que cuando se compra un módulo de seguridad prepagado, este módulo no funciona. Esto representa un inconveniente para el usuario que, a pesar de su compra, no puede tener acceso inmediato al servicio por el que ha pagado.

[0006] Con el fin de paliar este inconveniente, es factible enviar mensajes de autorización EMM para la activación de los módulos de seguridad, según intervalos temporales muy cortos, el usuario deberá esperar hasta que su módulo haya recibido tal mensaje. Esto presenta, sin embargo, el inconveniente de que utiliza un ancho de banda importante, que no siempre está disponible y que es costoso para el proveedor de datos.

[0007] Por supuesto, es posible introducir derechos de descifrado en el momento de la personalización del módulo de seguridad, es decir al final del proceso de fabricación, antes de que este módulo se ponga a la venta. Esto tendría el efecto hacer que la tarjeta fuera inmediatamente funcional en el momento de su introducción en el descodificador. Este procedimiento, sin embargo, no se pone en práctica casi nunca en realidad. De hecho, en caso de robo de los módulos de seguridad, por ejemplo, sería necesario enviar mensajes de autorización EMM que contuvieran, por una parte, un identificador de los módulos robados y, por otra parte, un control de desactivación, con objeto de hacer que estos módulos robados no fueran operativos. El tratamiento de tales mensajes de autorización EMM se puede bloquear de forma relativamente fácil. Sería por lo tanto difícil, incluso imposible, desactivar los módulos robados.

[0008] Hay por lo tanto una incompatibilidad entre el funcionamiento inmediato del módulo de seguridad desde su introducción en un descodificador y la capacidad de desactivar un módulo de seguridad robado o desactivar por otros motivos.

[0009] El resumen japonés JP 2004186714 describe un conjunto de descodificador/módulo de seguridad que funciona de la siguiente manera: se envía al descodificador un mensaje de autorización EMM que contiene un número de mensajes de control ECM autorizados. Este número de mensajes se graba en el módulo de seguridad. Este módulo de seguridad incluye una función de recuento que resta un valor del contador cada vez que se descifra un mensaje de control ECM.

[0010] Esta forma de realización presenta varios inconvenientes. En primer lugar, el contador recibe un número de mensajes de control que está autorizado a descifrar en un mensaje de autorización. Cuando se introduce un módulo de seguridad en un descodificador, es necesario por lo tanto esperar a la recepción y el tratamiento de un mensaje de autorización EMM antes de que el descodificador sea funcional. Esta invención no permite, por lo tanto, realizar un módulo de seguridad que funcione desde su introducción en un descodificador.

[0011] A continuación, cuando el valor del contador se ha introducido en el módulo de seguridad, sólo es posible desactivar el descodificador mandando un mensaje de autorización EMM que rescinda los derechos. O, de manera bien conocida, es relativamente fácil filtrar estos mensajes y eliminarlos antes de que los derechos hayan podido ser rescindidos. Así, un módulo de seguridad sólo se desactivará cuando el número de mensajes de control que esté autorizado a descifrar se haya alcanzado, siendo esta rescisión entonces automática. Esta invención no permite por lo tanto realizar un módulo de seguridad que se pueda desactivar muy rápidamente a voluntad.

[0012] La presente invención se propone realizar un módulo de seguridad que sea inmediatamente operativo, en el momento de su introducción en cualquier descodificador apropiado, sin inscripción previa en un centro de gestión. Se propone también dejar a un operador la posibilidad de desactivar uno o varios módulos de seguridad, en particular en caso de robos de módulos o en acaso de que ciertos módulos se utilicen de manera no autorizada.

Descripción de la invención

[0013] Los objetivos de la invención se alcanzan mediante un procedimiento caracterizado por el hecho de que incluye una etapa inicial de personalización del módulo de seguridad, en la que los derechos se introducen en un contador del módulo de seguridad, este procedimiento incluye además las etapas siguientes:

- recepción en la unidad multimedia de un mensaje de control ECM que contiene al menos una contraseña de control cw;
- transmisión de este mensaje ECM a dicho módulo de seguridad, este mensaje de control está asociado a un derecho de descifrado de los mensajes;
- lectura de un valor contenido en dicho contador del módulo de seguridad;
- comparación de este valor del contador para determinar si este valor está dentro de un rango que autoriza el descifrado;

    - en caso negativo, bloqueo del acceso en dichas datos con acceso condicional;
    - en caso afirmativo, descifrado del mensaje de control ECM y envío de la contraseña de control cw a dicha unidad multimedia;
    - determinación de una fecha de validez de los derechos de descifrado de los mensajes de control ECM asociados a dicho módulo de seguridad;
    - determinación de la fecha actual;
    - comparación de la fecha actual con la fecha de caducidad de los derechos de descifrado y determinación de si la fecha actual es anterior a la fecha de caducidad;

        - en caso afirmativo, autorización de acceso a los datos con acceso condicional;
        - en caso negativo, modificación del valor del contador según una regla preestablecida y autorización de acceso a los datos con acceso condicional.

[0014] Los objetivos de la invención se alcanzan además mediante un módulo de seguridad tal y como se define en el preámbulo y caracterizado por el hecho de que incluye medios para la ejecución del procedimiento tal y como se ha definido anteriormente.

[0015] Según esta invención, en el momento de la personalización de los módulos de seguridad, los derechos se introducen en estos módulos. Estos derechos permiten a los módulos funcionar desde su primera introducción en un descodificador. Estos derechos están, sin embargo, limitados, de manera que no ofrecen acceso a la totalidad de las capacidades del módulo de seguridad. De una forma más particular, los derechos están limitados en el tiempo.

[0016] De esta manera, si el módulo de seguridad no está en comunicación con un centro de gestión encargado de la transmisión de los derechos, el módulo de seguridad podrá únicamente funcionar de manera limitada. Para poder funcionar utilizando las capacidades que han sido previstas, será necesario permitir una comunicación entre el centro de gestión y el módulo de seguridad.

[0017] Esto permite al operador impedir el acceso a los datos por medio de módulos de seguridad que han sido robados o que se utilizan de manera ilegal. Este bloqueo del acceso a los datos puede hacerse de manera activa, mandando un mensaje de bloqueo en forma de mensaje de gestión EMM. El bloqueo puede hacerse también de manera pasiva, no renovando los derechos de descifrado. Así, si los mensajes de gestión se bloquean con el objetivo de eliminar las instrucciones de bloqueo para un módulo de seguridad, este bloqueo se hará, a pesar de todo, de manera pasiva.

[0018] El contador permite por lo tanto al módulo funcionar desde su introducción en un descodificador, para satisfacer al usuario. Esto permite al módulo esperar a la recepción de un mensaje de gestión EMM que renueve los derechos. La principal ventaja de este contador es que puede aumentar la duración del ciclo entre dos de estos mensajes de gestiones EMM y, por lo tanto, salvaguardar el ancho de banda, costoso para el operador de televisión de pago. Esto se realiza sin penalizar al usuario.

[0019] La inicialización de este contador en el momento de la personalización del módulo permite el funcionamiento de este módulo sin retardo, en el momento de la primera utilización, hasta la recepción del primer mensaje de gestión EMM.

[0020] La actualización del contador al mismo tiempo que la actualización de la fecha de validez intermedia permite el funcionamiento del módulo sin retardo en el momento de utilizaciones posteriores del módulo hasta la recepción de un próximo mensaje de gestión EMM. Esto permite no penalizar a los usuarios insertando un módulo después de un largo período fuera de la unidad multimedia.

[0021] El hecho de enviar el valor del contador en los mensajes de gestión EMM permite modificar este valor en función de las restricciones operativas. Se puede, por ejemplo, aumentar este valor si el ancho de banda disponible para los mensajes de gestión EMM disminuye.

Breve descripción de los dibujos

[0022] La presente invención y sus ventajas se entenderán mejor en referencia al dibujo anexo y a la descripción detallada de una forma de realización particular, en la que:

- la figura 1 ilustra una variante del procedimiento de la invención.

Manera de realizar la invención

[0023] En referencia a la figura 1, el procedimiento de la invención se explica en una aplicación particular con relación a la televisión con acceso condicional. En esta aplicación, un centro de gestión envía los datos con acceso condicional a una pluralidad de unidades multimedia que comporta cada una un descodificador y un módulo de seguridad. En la aplicación considerada, el módulo de seguridad es del tipo desmontable y puede estar realizado, en particular, en forma de tarjeta inteligente. El módulo incluye particularmente un contador cuya función se explica más adelante.

[0024] De manera convencional, los datos con acceso condicional tales como los enviados por el centro de gestión forman un contenido de televisión de pago. Estos datos se cifran mediante contraseñas de control cw. Las contraseñas de control cw son ellas mismas cifradas y mandadas a los usuarios en cuestión en forma de mensajes de control ECM. Los derechos de acceso al contenido cifrado se pueden mandar a las unidades multimedia de los usuarios en forma de mensajes de autorización EMM.

[0025] Cuando un usuario desea tener acceso a un contenido cifrado, los mensajes de control recibidos por el descodificador de este usuario se transmiten al módulo de seguridad de la unidad multimedia en cuestión. El módulo de seguridad verifica en primer lugar si dispone de los derechos requeridos para acceder al contenido. Si tal es el caso, el módulo de seguridad descifra los mensajes de control ECM para extraer las contraseñas de control cw. Éstas se devuelven entonces al descodificador, que las utiliza para descifrar el contenido.

[0026] Como se ha indicado anteriormente, el módulo de seguridad según la presente invención contiene un contador. Se introduce un valor predeterminado en este contador en el momento de la personalización. Este valor puede ser un valor digital o una duración determinada. Este módulo de seguridad contiene igualmente una fecha de caducidad final que no se puede modificar y que es la fecha más allá de la cual este módulo ya no podrá funcionar. Contiene también un registro previsto para recibir una fecha de validez intermedia. En el momento de la personalización, este registro se puede dejar vacío. Sin embargo, también es posible introducir una fecha en la personalización, esta fecha puede ser, por ejemplo, la fecha de la personalización o una fecha relativamente cercana.

[0027] El módulo de seguridad puede además contener un crédito que representa una suma de dinero cargada en este módulo. Este crédito se carga igualmente en el momento de la personalización o posteriormente, por ejemplo en el momento en el que un usuario realiza la compra del módulo.

[0028] Cuando un usuario ha adquirido un módulo de seguridad para tener acceso a un contenido de televisión de pago, puede introducir este módulo en cualquier descodificador adecuado.

[0029] En la práctica, es habitual utilizar un valor digital que no sea nulo, por ejemplo 180, como valor inicial del contador e ir restando 1 unidad al valor del contador en el momento de cada descifrado. En caso del criptoperiodo, es decir el intervalo entre dos cambios sucesivos de contraseñas de control es de 10 segundos, el valor de 180 corresponda al descifrado de 1800 segundos, sea 30 minutos de contenido. Como se indica anteriormente, el valor de contador puede ser igualmente una duración, por ejemplo 30 minutos. En tal caso, el tiempo de descifrado autorizado es independiente del criptoperiodo. En cambio, es necesario utilizar medios de medida del tiempo diferentes del recuento del número de mensajes de control ECM descifrados. Estos medios pueden particularmente utilizar un reloj dispuesto en el descodificador o el tiempo absoluto enviado por el centro de gestión. En tal caso, la hora de inicio del descifrado de un mensaje de control se memoriza. En el momento de cada descifrado, se calcula la duración entre esta hora de inicio de

descifrado y la hora actual. Esta duración se compara a continuación con la duración contenida en el contador. El acceso a los datos se autoriza únicamente si la duración calculada es inferior a la duración memorizada en el contador.

[0030] El centro de gestión envía a intervalos regulares un mensaje de autorización EMM que contiene una fecha de validez intermedia. Según una forma de realización preferida, los mensajes de autorización EMM contienen uno o varios rangos de números de identificación de los módulos de seguridad a los que se debe enviar una fecha de validez intermedia y un valor de contador. Los módulos de seguridad cuyo número de identificación no figura en ninguno de los rangos de los mensajes de autorización no reciben por lo tanto una nueva fecha de validez intermedia y el contador no se reinicia. De esta manera, los módulos de seguridad cuyo número único de identificación no está contenido en un mensaje de autorización EMM se desactivan de manera pasiva.

[0031] Se debe señalar que, en función del tamaño de los mensajes de autorización EMM y del espacio necesario para enviar todos los rangos en cuestión, es posible generar uno solo o, por el contrario, varios mensajes de autorización EMM. Estos mensajes se pueden enviar a grupos de módulos de seguridad o a todos los módulos. Según una variante, los mensajes de autorización EMM se pueden enviar individualmente, utilizando números de identificación únicos de los módulos de seguridad.

[0032] Cuando tal mensaje de autorización EMM es recibido por una unidad multimedia de un usuario, éste se descifra para extraer, por una parte, la fecha de validez intermedia y, por otra parte, el nuevo valor de contador. Estos dos datos se memorizan en las ubicaciones adecuadas del módulo de seguridad.

[0033] Según una variante de realización, el valor del contador podría ser nulo al principio e incrementar en el momento de los descifrados. El bloqueo se efectuaría entonces cuando el contador alcanzara un límite predeterminado. También es posible restar al contador valores diferentes en función de los contenidos difundidos. Al contador se le podría restar una unidad en el momento de la difusión de una película y dos unidades en el momento de la difusión de un encuentro deportivo.

[0034] Según la forma de realización ilustrada por la figura 1, el procedimiento comienza por una etapa 114 de lectura del valor contenido en el contador. Esta etapa es seguida de una etapa 115 cuyo objetivo es determinar si el valor del contador está dentro del rango de descifrado autorizado, es decir que este valor sea superior a 0. Si este valor está fuera del rango de descifrado autorizado, o en nuestro ejemplo, si es nulo, el acceso a los datos se prohíbe, lo que se ilustra por una etapa 116. Si este valor no es nulo, la contraseña de control se descifra en una etapa 112. La fecha de validez intermedia se lee a continuación en el momento de una etapa 110 y se compara con la fecha actual en la etapa 111. Si la fecha actual es posterior a la fecha de validez intermedia, al contador se le resta según la regla preestablecida, correspondiente a la etapa 117. Si no, este valor del contador no se modifica y el acceso a los datos se autoriza. Como se ha indicado anteriormente, el módulo de seguridad puede contener también un crédito. El procedimiento de la invención puede igualmente comportar, antes de cualquier otro proceso, una etapa de verificación del crédito restante en el módulo. Esta verificación se efectúa de la siguiente manera. Cuando un usuario indica que desea tener acceso a un contenido determinado al que está asociado un importe predefinido, el módulo verifica si contiene un crédito superior o igual al importe asociado al contenido solicitado. Si tal es el caso, se inicia el procedimiento tal y como se ha explicado previamente. Si este procedimiento llega al descifrado de los datos, al crédito se le resta la cantidad asociada al evento y el nuevo crédito se memoriza.

[0035] Si el procedimiento correspondiente a las etapas referenciadas de 110 a 116 no llega al descifrado de los datos, el crédito no se modifica.

[0036] Si el crédito inicial es inferior a la cantidad asociada al contenido requerido, el derecho de acceso al evento no se da y el contenido no se puede visualizar. Según la forma de realización elegida, es posible permitir la carga de un crédito suplementario en el módulo de seguridad o al contrario, impedir esta carga.

REIVINDICACIONES

1. Procedimiento de control de acceso a datos con acceso condicional en una unidad multimedia que comporta al menos un módulo de seguridad, **caracterizado por el hecho de que** incluye una etapa inicial de personalización del módulo de seguridad en la cual los derechos se introducen en un contador del módulo de seguridad, este procedimiento comporta además las etapas siguientes:

- recepción por la unidad multimedia de un mensaje de control ECM que contiene al menos una contraseña de control cw;

- transmisión de este mensaje ECM a dicho módulo de seguridad, este mensaje de control está asociado a un derecho de descifrado de los mensajes;

- lectura de un valor contenido en dicho contador del módulo de seguridad;

- comparación de este valor del contador con un rango de valores que autoriza el descifrado para determinar si este valor está comprendido dentro de este rango de valores;

- en caso negativo, bloqueo del acceso a dichos datos con acceso condicional;

- en caso afirmativo, descifrado del mensaje de control ECM en el módulo de seguridad y envío de la contraseña de control cw desde el módulo de seguridad a dicha unidad multimedia;

- determinación de una fecha de validez de los derechos de descifrado de los mensajes de control ECM asociados a dicho módulo de seguridad;

- determinación de la fecha actual;

- comparación de la fecha actual con la fecha de caducidad de los derechos de descifrado y determinación de si la fecha actual es anterior a la fecha de expiración;

- en caso afirmativo, autorización de acceso a los datos con acceso condicional;

- en caso contrario, modificación del valor del contador según una regla preestablecida y autorización de acceso a los datos con acceso condicional.

2. Procedimiento según la reivindicación 1, **caracterizado por el hecho de que** la unidad multimedia recibe, según intervalos de tiempo predefinidos, un mensaje de autorización EMM con una fecha de validez, esta fecha de validez es posterior a la fecha actual, esta fecha de validez se memoriza en el módulo de seguridad.

3. Procedimiento según la reivindicación 2, **caracterizado por el hecho de que** el mensaje de autorización EMM incluye además un nuevo valor de contador que se debe introducir en el contador del módulo de seguridad.

4. Procedimiento según la reivindicación 3, **caracterizado por el hecho de que** el nuevo valor de contador que se debe introducir en el contador es un valor digital, este valor digital está unido al número de mensajes de control ECM que el módulo de seguridad está autorizado a descifrar.

5. Procedimiento según la reivindicación 3, **caracterizado por el hecho de que** el valor que se debe introducir en el contador es una duración, esta duración es la duración del contenido que el módulo de seguridad está autorizado a descifrar.

6. Procedimiento según la reivindicación 1, **caracterizado por el hecho de que** el rango de valores que autoriza el descifrado está comprendido entre 1 y un valor de umbral superior a 1, los límites de este margen están comprendidos en el rango, y por el hecho de que la regla preestablecida para la modificación del valor del contador consiste en disminuir este valor.

7. Procedimiento según la reivindicación 6, **caracterizado por el hecho de que** el valor del contador se disminuye en por lo menos una unidad cada vez que un mensaje de control ECM se descifra.

8. Procedimiento según la reivindicación 7, **caracterizado por el hecho de que** el valor del contador se disminuye en un número de unidades dependiendo del contenido asociado a los mensajes de control ECM descifrados.

9. Módulo de seguridad para el acceso a datos con acceso condicional, **caracterizado por el hecho de que** incluye medios para la ejecución del procedimiento de la reivindicación 1.

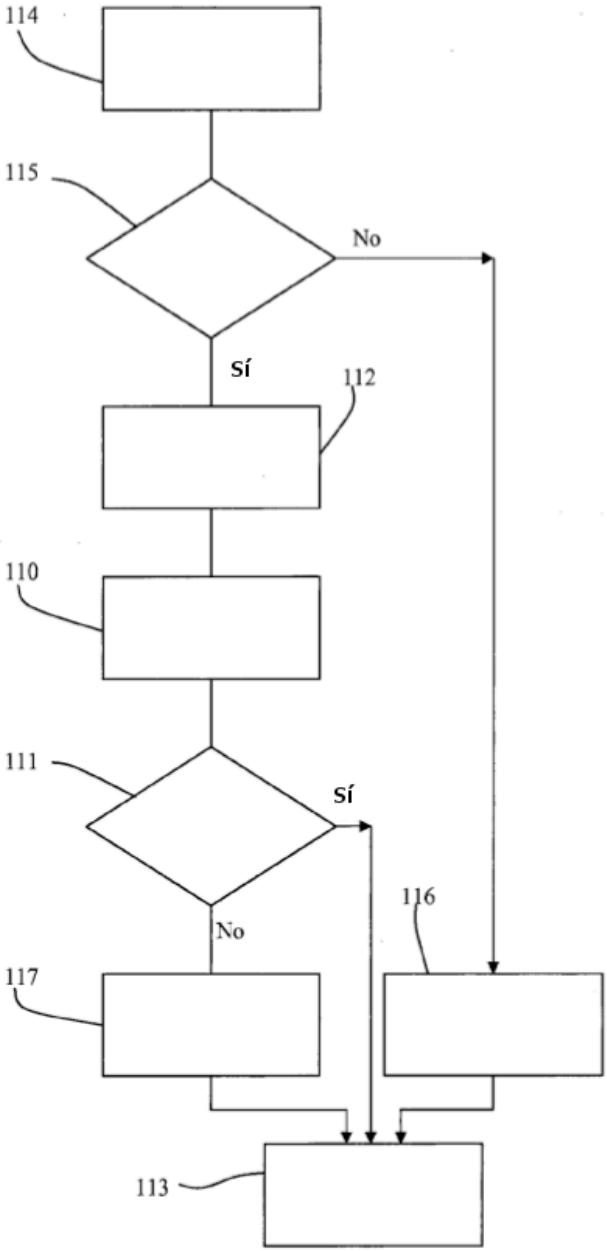

FIG. 1