



(19)



OFICINA ESPAÑOLA DE
PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 342 375**

(51) Int. Cl.:
H04L 29/06 (2006.01)

(12)

TRADUCCIÓN DE PATENTE EUROPEA

T3

(96) Número de solicitud europea: **03727574 .0**

(96) Fecha de presentación : **06.03.2003**

(97) Número de publicación de la solicitud: **1483877**

(97) Fecha de publicación de la solicitud: **08.12.2004**

(54) Título: **Protocolo de inscripción, de invalidación y/o de borrado de derechos de acceso a informaciones encriptadas y módulo de control de acceso correspondiente.**

(30) Prioridad: **08.03.2002 FR 02 02969**

(45) Fecha de publicación de la mención BOPI:
06.07.2010

(45) Fecha de la publicación del folleto de la patente:
06.07.2010

(73) Titular/es: **Viaccess
Les Collines de l'Arche, Tour Opera C
92057 Paris La Defense, FR**

(72) Inventor/es: **Becker, Claudia;
Codet, André;
Fevrier, Pierre y
Guionnet, Chantal**

(74) Agente: **Espiell Volart, Eduardo María**

ES 2 342 375 T3

Aviso: En el plazo de nueve meses a contar desde la fecha de publicación en el Boletín europeo de patentes, de la mención de concesión de la patente europea, cualquier persona podrá oponerse ante la Oficina Europea de Patentes a la patente concedida. La oposición deberá formularse por escrito y estar motivada; sólo se considerará como formulada una vez que se haya realizado el pago de la tasa de oposición (art. 99.1 del Convenio sobre concesión de Patentes Europeas).

DESCRIPCIÓN

Protocolo de inscripción, de invalidación y/o de borrado de derechos de acceso a informaciones encriptadas y módulo de control de acceso correspondiente.

Los protocolos de inscripción, de invalidación y/o de borrado de derechos de acceso a informaciones encriptadas tienen, en el momento actual, una importancia primordial para asegurar una gestión más fluida y más flexible posible de las prestaciones de servicio en el dominio del control de acceso a las informaciones encriptadas.

En esta descripción, los términos “protocolo” y “procedimiento” se consideran sinónimos.

En particular el caso del dominio de la televisión de pago es el dominio en el cual los servicios o prestaciones de servicios propuestos tienden a cubrir los servicios y prestaciones más diversos.

En particular, en el dominio citado anteriormente, la renovación periódica de los abonos de un abonado se efectúa por la adición, o inscripción, de una nueva información característica de la prolongación o del nuevo abono suscrito por el abonado.

Con motivo de la independencia de la gestión de los derechos de acceso suscritos y atribuidos a cada abonado y del control de acceso propiamente dicho, efectuándose la gestión de los derechos de acceso por medio de mensajes de gestión, llamados mensajes EMM, que pueden transportar los derechos de acceso y efectuándose el control de acceso mediante la difusión de mensajes de control de acceso, llamados mensajes ECM, que comprenden una palabra de control de acceso cifrado, que desempeña el papel de una clave de servicio y de los criterios de acceso, una renovación semejante se traduce por medio de la inscripción, en la memoria del procesador de seguridad asociado al decodificador o al módulo de control de acceso, de una nueva información.

Estando el módulo de control de acceso constituido, de manera habitual, por una tarjeta con microprocesador, del tipo tarjeta bancaria, los recursos en memoria de este último son necesariamente limitados.

Por esta razón, el procedimiento citado anteriormente de inscripción de derechos está dotado de una función de borrado de los derechos caducados. Esta última tiene, sin embargo, como único fin liberar el espacio de memoria en el módulo de control de acceso o la tarjeta, con el fin de evitar, al final, su saturación.

Un procedimiento semejante de inscripción/borrado no permite asegurar, con toda la flexibilidad y la seguridad necesarias, una gestión fluida de los derechos de acceso inscritos en el módulo de control de acceso o la tarjeta atribuida a cada abonado.

Esto sucede, por ejemplo, después de un impago del abonado, o incluso en el marco de ofertas modulables durante el cambio, por el abonado, de la oferta a la que se ha suscrito este último.

Debido al criterio de seguridad, en razón del carácter un poco tosco del procedimiento actual de borrado, todo abonado deshonesto tiene la posibilidad de filtrar e interceptar los mensajes de borrado que tendrían por objeto reducir o controlar los derechos de acceso de este último.

Además, no puede excluirse un procedimiento de grabación de los mensajes EMM de inscripción de derechos con vistas a someter estos últimos de manera ilícita a un procedimiento de reasignación.

Finalmente, los procedimientos actuales de inscripción y/o de borrado de derechos por mensajes EMM pueden provocar una disfunción de estas operaciones, relacionada con la falta de respeto a una secuenciación adaptada.

Se conoce otro estado de la técnica a través del artículo de D. VAN SCHOONEVELD, “Standardization of conditional access systems for digital pay television”, Philips Journal of Research, Volumen 50 (1996) 217-225, XP004008213.

La presente invención tiene por objeto la puesta en práctica de un protocolo de inscripción, de invalidación y/o de borrado de derechos de acceso a las informaciones encriptadas que permite, por una parte, asegurar un control y una gestión de los derechos de acceso inscritos con una flexibilidad muy grande y con una fluidez muy grande, y, por otra parte, mejorar sustancialmente el nivel de seguridad ofrecido.

En particular, un objeto de la presente invención es la puesta en práctica de un protocolo de inscripción, de invalidación y/o de borrado de derechos de acceso a las informaciones encriptadas, en el que cada operación de inscripción, de invalidación y/o de borrado se hace condicionada a una referencia anterior, como una fecha de acción.

Otro objeto de la presente invención es asimismo la puesta en práctica de un protocolo de inscripción, de invalidación y/o de borrado de derechos de acceso a las informaciones encriptadas en el que las operaciones de inscripción, de invalidación y/o de borrado de derechos de acceso pueden codificarse, con el fin de mejorar la seguridad y de impedir toda reasignación de los mensajes de orden interceptados correspondientes.

Otro objeto de la presente invención es, finalmente, la puesta en práctica de un módulo de control de acceso que permite la inscripción, en la memoria programable de este último, de los derechos de acceso y de monederos electrónicos que permiten la puesta en práctica del protocolo objeto de la presente invención.

- 5 La invención tiene así por objeto un procedimiento de inscripción, de invalidación y/o de borrado de derechos de acceso de informaciones encriptadas conforme a la reivindicación 1.

La invención tiene igualmente por objeto un módulo de control de acceso conforme a la reivindicación 14.

- 10 El protocolo y el módulo de control de acceso, objetos de la presente invención, encuentran aplicación, no sólo en la transmisión punto-multipunto de datos encriptados, en particular en la televisión de pago, sino igualmente en la transmisión punto a punto de datos de imágenes de vídeo o de ejecución de servicios, en red, según el protocolo IP, por ejemplo.

- 15 Se comprenderán mejor con la lectura de la descripción y con la observación de los dibujos indicados a continuación, en los cuales:

la fig. 1 representa, a título ilustrativo, un organigrama general de las etapas que permiten la puesta en práctica del protocolo objeto de la presente invención;

- 20 la fig. 2a representa, a título ilustrativo, un organigrama específico de las etapas que permiten la puesta en práctica del protocolo objeto de la presente invención, durante una operación de inscripción de un derecho válido, en el módulo de control de acceso atribuido a un abonado;

- 25 la fig. 2b representa, a título indicativo, un organigrama específico de las etapas que permiten la puesta en práctica del protocolo objeto de la presente invención, durante una operación de invalidación de un derecho inscrito en el módulo de control de acceso atribuido a un abonado;

- 30 la fig. 2c representa, a título ilustrativo, un organigrama específico de las etapas que permiten la puesta en práctica del protocolo objeto de la presente invención, durante una operación de borrado de un derecho de acceso inscrito, correspondiendo la operación de borrado a un borrado virtual, en razón del carácter momentáneamente diferido del borrado físico de este derecho;

- 35 la fig. 2d representa, a título ilustrativo, un organigrama específico de la introducción de un borrado físico de un derecho de acceso inscrito, condicionado a un criterio específico, tal como, por ejemplo, un criterio temporal;

las fig. 3a y 3b representan un módulo de control de acceso según la invención.

- 40 A continuación se dará una descripción más detallada del protocolo de inscripción, de invalidación y/o de borrado de derechos de acceso a unas informaciones encriptadas, conforme al objeto de la presente invención, en relación con la fig. 1 y las figuras siguientes.

- 45 De una manera general, se recuerda que el protocolo, objeto de la presente invención, permite gestionar los derechos de acceso a informaciones encriptadas transmitidas de un centro de emisión hacia una pluralidad de terminales de descifrado. A cada terminal T_k se le asocia un módulo de control de acceso provisto de un procesador de seguridad.

- 50 De manera clásica, cada módulo de control de acceso puede estar constituido por una tarjeta con microprocesador que contiene el procesador de seguridad citado anteriormente, así como por las memorias seguras que permiten la memorización de las claves de desciframiento y, finalmente, toda operación de verificación de autenticidad, por ejemplo. Cada módulo de control de acceso está dotado de una memoria no volátil programable y los derechos de acceso a las informaciones encriptadas están inscritos en el módulo de control de acceso, en la memoria no volátil programable citada anteriormente.

- 55 Las informaciones encriptadas se someten a un control de acceso por emisión periódica de mensajes de control de acceso, mensajes denominados mensajes ECM. Estos mensajes de control de acceso son portadores de criterios de acceso y de un criptograma de una palabra de control cambiada periódicamente y cifrada por medio de una clave de explotación.

- 60 En cada procesador de seguridad, condicionado a la verificación del valor verdadero de al menos un derecho de acceso inscrito con respecto a criterios de acceso transportados por los mensajes de control de acceso, el control de acceso se efectúa por desciframiento del criptograma de la palabra de control a partir de la clave de explotación, memorizada en la memoria no volátil segura del procesador de seguridad, por transmisión al terminal de descifrado de la palabra de control restituida por el módulo de control de acceso, y después descifrado de las informaciones encriptadas a partir de la palabra de control restituida en el terminal de descifrado citado anteriormente.

En el marco de un procedimiento de control de acceso a las informaciones encriptadas citadas anteriormente, el protocolo, objeto de la presente invención, es notable porque consiste al menos en constituir y definir todo derecho

ES 2 342 375 T3

de acceso inscrito en el módulo de control de acceso como un conjunto de variables independientes y de variables relacionadas. Estas variables incluyen al menos, además de una variable de identificación del derecho de acceso y una variable de fechas de validez, una variable de fecha de acción en el derecho de acceso inscrito en el módulo de control de acceso y una variable de estado que puede tomar uno de tres valores codificados, es decir, derecho de acceso válido, derecho de acceso invalidado o incluso derecho de acceso borrado.

En referencia a la fig. 1 citada anteriormente, se designa por:

- R_ID: variable de identificación de derecho de acceso;
- V_D: variable de fechas de validez;
- AD_V: variable de fecha de acción en el derecho de acceso inscrito;
- S_V: variable de estado que puede tomar uno de los tres valores codificados, derecho de acceso válido, derecho de acceso invalidado o derecho de acceso borrado.

A título de ejemplo no limitativo, se indica que los tres valores codificados pueden corresponder a:

- S_V = 0 para un derecho invalidado;
- S_V = 1 para un derecho válido;
- S_V = 2 para un derecho borrado.

Teniendo en cuenta las consideraciones precedentes, se comprende, naturalmente, que la definición y la constitución de los derechos de acceso, tal como se menciona anteriormente en la descripción, son esenciales para la puesta en práctica del protocolo objeto de la presente invención. Esta etapa se representa en la etapa 0 de la fig. 1 y cada derecho de acceso AR puede corresponder entonces a la sintaxis mostrada a continuación:

$$AR = [V_D] R_ID [R_SID] AD_V S_V \quad (1)$$

En referencia a la relación citada anteriormente, se indica que, conforme a la codificación específica de los derechos de acceso citados anteriormente, toda variable entre corchetes se considera opcional.

Dado que la variable de fechas de validez V_D es una variable independiente, puede hacerse opcional por razones de codificación específica, pudiendo corresponder la ausencia de variable de fechas de validez, para un derecho de acceso inscrito, por ejemplo, para un valor particular de este derecho.

Por el contrario, la variable R_SID, variable de subidentificación de derecho, es una variable relacionada con la variable de identificación de derecho de acceso R_ID.

En estas condiciones, se considera la presencia de las variables independientes de identificación de derecho de acceso R_ID, de fecha de acción AD_V y de variable de estado S_V como necesaria para la puesta en práctica del protocolo objeto de la presente invención, implementándose este último esencialmente para derechos de acceso inscritos e incluyendo, si bien de manera opcional, una variable de fecha de validez.

Así, en referencia a la relación (1) precedente, se indica que para estas variables:

- V_D: indica un intervalo de fecha de validez, el cual puede ser fijo y estar representado por una fecha de inicio y una fecha de fin de derecho de acceso, o deslizante y definido entonces en número de días, llegado el caso por una fecha de caducidad. Entonces, el intervalo de validez puede transformarse en valor fijo en la primera utilización, por ejemplo.
- R_ID y R_SID: las variables citadas anteriormente corresponden a los identificadores y subidentificadores del derecho inscrito y permiten, naturalmente, referenciar este derecho en los criterios de acceso transportados por los mensajes de control de acceso ECM.
- AD_V: indica la fecha en la cual se ha efectuado una operación en el derecho inscrito. De una manera más específica, se indica que la variable citada anteriormente indica ya sea la fecha de inscripción del derecho inscrito en la tarjeta cuando no se ha efectuado ninguna operación en este último, o bien al contrario, la fecha de ejecución, fecha de acción, de la última operación posterior y, en particular, la fecha de actualización, la fecha de invalidación o incluso la fecha de borrado, tal y como se describirá posteriormente en la descripción.

- S_V: indica el valor codificado de la variable de estado. En referencia a la fig. 1, se indica que esta variable codificada puede tomar los valores 0, 1, 2 citados anteriormente o cualquier otro valor, por ejemplo, explícito o cifrado.

5

En referencia a la fig. 1, se considera la etapa de constitución y de definición de los derechos de acceso, tal como se menciona anteriormente, como realizada.

Después de la etapa 0 citada anteriormente, el protocolo, objeto de la presente invención, consiste en una etapa A, en transmitir, desde el centro de emisión hacia cada terminal de descifrado T_k y, naturalmente, hacia el módulo de control de acceso asociado a este último, al menos un mensaje de gestión de derechos de acceso denominado mensaje EXM.

Este mensaje incluye, tal y como se representa en la fig. 1, al menos una variable de identificación de derechos de acceso inscritos, denominándose esta variable R_{ID_x} , una variable de fecha de acción denominada AD_{V_x} , correspondiendo esta fecha de acción a la fecha de emisión del mensaje de gestión, es decir, la fecha de operación de gestión realizada en el derecho de acceso inscrito cuya variable de identificación R_{ID} corresponde a la variable de identificación R_{ID_x} contenida en el mensaje de gestión, tal y como se explicará a continuación en la descripción. El mensaje puede, además, incluir una variable de fechas de validez, denominada V_{D_x} . Finalmente, el mensaje de gestión EXM comprende una variable de asignación de estado notada S_{V_x} constituida por un valor codificado correspondiente a un derecho de acceso válido, un derecho de acceso invalidado o un derecho de acceso borrado. La variable S_{V_x} puede tomar así los valores 0, 1, 2, tal y como se ha mencionado anteriormente en la descripción.

En recepción del mensaje de gestión EXM en el módulo de control de acceso asociado al terminal de descifrado, el protocolo, objeto de la invención, consiste, en una etapa B, en asignar al derecho de acceso inscrito correspondiente a la variable de identificación de derecho de acceso del mensaje de gestión de derechos de acceso la fecha de acción, y después, en una etapa C, en asignar a la variable de estado S_V del derecho de acceso inscrito, la variable de asignación de estado S_{V_x} correspondiente a un derecho de acceso válido, a un derecho de acceso invalidado o a un derecho de acceso borrado.

30

En lo que concierne a la puesta en práctica de la etapa B, se indica que esta etapa puede realizarse mediante la puesta en práctica de una orden de tipo lógico If (Si)... Then (Entonces).

En estas condiciones, la etapa B citada anteriormente, tal y como se representa en la fig. 1, puede consistir en comparar el valor de la variable de identificación del derecho de acceso inscrito R_{ID} con la variable de identificación de derechos de acceso inscritos contenidos en el mensaje de gestión EXM, es decir, con la variable R_{ID_x} por comparación de igualdad. La comparación de igualdad citada anteriormente puede incluir una pluralidad de comparaciones sucesivas que se aplican a las variables tales como la variable de subidentificación del derecho R_{SID} y la variable de fechas de validez, llegado el caso en cualquier otra variable.

40

Cuando se verifica esta igualdad, entonces, a la variable de fecha de acción AD_V se le atribuye, bajo condición, el valor de la variable de fecha de acción AD_{V_x} del mensaje de gestión EXM. La condición citada anteriormente consiste en verificar la posterioridad de la variable AD_{V_x} con respecto a la variable AD_V . Después, a la variable de estado del derecho de acceso inscrito S_V se le atribuye la variable de asignación de estado S_{V_x} contenida en el mensaje de gestión EXM. Esta operación se realiza, en la etapa C, por instanciación de la variable de estado del derecho de acceso inscrito S_V representada por la igualdad:

45

$$S_V = S_{V_x}$$

50

A continuación se dará una descripción más detallada de la puesta en práctica del protocolo objeto de la presente invención, en el marco de operaciones de inscripción de un derecho válido, de invalidación de un derecho y después de borrado de un derecho inscrito, en relación con las fig. 2a a 2d.

Para una operación de inscripción de un derecho de acceso determinado en un módulo de control de acceso, la variable de fecha de acción AD_{V_x} , en el mensaje EXM de gestión, corresponde a una fecha de inscripción de este derecho de acceso y la variable de asignación S_{V_x} es un valor codificado correspondiente a un derecho válido, es decir, al valor codificado $S_{V_x} = 1$.

La operación de inscripción propiamente dicha del derecho de acceso consiste en inscribir, en el módulo de control de acceso, y en particular en la memoria no volátil de este último, un derecho de acceso determinado cuya fecha de acción es la de la fecha de inscripción citada anteriormente y cuya variable de estado es la de la variable de estado $S_{V_x} = 1$.

En referencia a la fig. 2a, la operación de inscripción se inicia por la recepción, en el terminal de descifrado T_k del mensaje EXM, en la etapa B_{0a} .

65

ES 2 342 375 T3

Se dispone, al nivel del módulo de control de acceso, después de demultiplexado del mensaje EXM, de las variables R_ID_x , V_D_x , AD_V_x , $S_V_x = 1$ extraídas del mensaje EXM y de las variables R_ID , V_D , AD_V , S_V del derecho inscrito en el módulo de control de acceso, si este último está efectivamente inscrito.

5 Para la operación de inscripción citada anteriormente, el protocolo objeto de la presente invención puede consistir, tal y como se representa en la fig. 2a, en verificar, en una etapa B_{1a} , la existencia de un derecho inscrito correspondiente. Esta prueba se indica como:

$$\exists R_ID = R_ID_x$$

10

Esta prueba se acompaña de una prueba de no pertenencia de este derecho al estado borrado, $S_V \neq 2$, con el fin de permitir la ejecución de la operación de inscripción para los derechos existentes en el estado invalidado o en el estado inscrito, en vista de una operación de reinscripción para lo que concierne a estos últimos. La prueba implementada en la etapa B_{1a} verifica la relación:

15

$$\exists R_ID = R_ID_x \text{ Y } S_V \neq 2$$

20 En respuesta positiva a la etapa B_{1a} , el protocolo objeto de la invención puede consistir en verificar el carácter de posterioridad de la variable de fecha de acción correspondiente a una fecha de inscripción con respecto a la fecha de acción del derecho de acceso correspondiente. Esta operación puede realizarse, en la etapa B_{2a} , por comparación de superioridad de la fecha de acción y de la variable de fecha de acción AD_V_x contenida en el mensaje EXM con respecto a la fecha de acción del derecho inscrito AD_V .

25

En respuesta negativa a la prueba de la etapa B_{2a} citada anteriormente, la operación de inscripción se termina por una etapa de fin de inscripción B_{3a} , no siendo efectiva la operación de inscripción del derecho.

30 Por el contrario, en respuesta positiva a la prueba de la etapa B_{2a} , esta última se sigue entonces de una etapa B_{4a} consistente en efectuar una actualización de la variable de fecha de acción del derecho de acceso correspondiente a partir de la fecha de acción correspondiente a una fecha de inscripción.

Esta operación se representa mediante la relación:

35

$$AD_V = AD_V_x$$

La etapa B_{4a} de actualización se sigue entonces de la etapa C de asignación consistente en asignar, a la variable de estado del derecho de acceso idéntico S_V , el valor codificado correspondiente a un derecho válido, por ejemplo $S_V_x = 1$. Entonces, el derecho de acceso inscrito previamente en el módulo de control de acceso se renueva o reactualiza.

40

El protocolo objeto de la presente invención para una operación de inscripción puede, naturalmente, ponerse en práctica para la ejecución de una primera inscripción de un derecho en un módulo de control de acceso.

45 En una situación semejante, no existe derecho inscrito correspondiente a la variable de identificación de derecho de acceso del mensaje EXM, variable R_ID_x , y la comparación de igualdad de la relación de la prueba realizada en la etapa B_{1a} no se verifica.

50 En consecuencia, en respuesta negativa a la prueba de la etapa citada anteriormente, respuesta negativa a la verificación de la relación $\exists R_ID = R_ID_x \text{ Y } S_V \neq 2$, el protocolo objeto de la invención consiste, además, en efectuar una actualización en primera inscripción de este derecho de acceso cuya fecha de acción corresponde a la fecha de inscripción.

55 Esta operación se representa, en la fig. 2a, mediante el acceso, en respuesta negativa a la etapa B_{1a} , a la etapa de actualización $AD_V = AD_V_x$.

60

Este acceso puede realizarse por asignación a la variable R_ID del derecho cuya inscripción se efectúa, en la etapa B_{5a} , del valor R_ID_x contenido en el mensaje de gestión EXM, y después en la etapa B_{6a} , de la variable de fechas de validez V_D_x a la variable de validez V_D .

La operación de asignación, en la etapa C, corresponde, en este caso, a una primera inscripción.

65 Asimismo, en referencia a la fig. 2a, para un derecho de acceso inscrito cuya variable de asignación de estado corresponde a un derecho borrado, pero siempre presente físicamente, $S_V = 2$, éste consiste igualmente en respuesta negativa a la prueba B_{1a} , ventajosamente, en efectuar una nueva inscripción del derecho, etapas B_{5a} , B_{6a} y B_{4a} . A este derecho de acceso inscrito se le asigna entonces una variable de estado correspondiente a un derecho válido, etapa C.

ES 2 342 375 T3

A continuación se describirá una descripción más detallada de una operación de invalidación de un derecho de acceso inscrito en un módulo de control de acceso conforme al protocolo objeto de la presente invención en relación con la fig. 2b.

5 En una situación semejante, la variable de fecha de acción del mensaje de gestión de derechos de acceso corresponde a una fecha de invalidación y la variable de asignación de estado S_V_x es el valor codificado correspondiente a un derecho invalidado, es decir, el valor cero en el ejemplo dado anteriormente en la descripción.

10 En estas condiciones, la operación de invalidación del derecho inscrito en el módulo de control de acceso consiste en asignar, a la variable de estado del derecho de acceso inscrito S_V , el valor codificado correspondiente a un derecho de acceso invalidado, es decir, el valor codificado $S_V_x = 0$ y, naturalmente, en actualizar la fecha de acción del derecho de acceso inscrito a partir de la fecha de invalidación.

15 Para este fin, tal y como se representa en la fig. 2b, la operación de invalidación se inicia mediante una etapa de recepción del mensaje EXM de gestión relativa a esta operación en el terminal de descryptado T_k .

20 Durante esta etapa, referida como B_{0b} en la fig. 2b, se disponen variables de identificación de derecho de acceso R_ID_x , de fechas de validez V_D_x , de fecha de acción AD_V_x y de variable de asignación de estado $S_V_x = 0$ contenidas en el mensaje EXM, así como variables de identificación de derecho R_ID , de fecha de validez V_D , de fecha de acción AD_V y de variable de estado S_V del derecho inscrito en el módulo de control de acceso.

25 En estas condiciones, el protocolo objeto de la presente invención puede consistir, tal y como se representa en la fig. 2b, previamente a la operación de invalidación propiamente dicha, en verificar, en una etapa B_{1b} , en el módulo de control de acceso, la existencia de un derecho de acceso inscrito correspondiente. La prueba B_{1b} es semejante a la prueba B_{1a} de la fig. 1a.

30 Además, y de manera no limitativa, esta operación de prueba puede consistir en verificar, al igual que en la prueba B_{1a} de la fig. 1a, que el derecho de acceso inscrito correspondiente es un derecho de acceso válido o inválido en el cual debe efectuarse la operación de invalidación.

35 Por este motivo, la prueba realizada en la etapa B_{1b} verifica la relación:

$$\exists R_ID = R_ID_x \text{ Y } S_V \neq 2$$

40 En respuesta positiva a la etapa B_{1b} , esta última puede entonces seguirse de una etapa B_{2b} consistente en verificar el carácter de posterioridad de la variable de fecha de acción correspondiente a una fecha de invalidación con respecto a la variable de fecha de acción del derecho inscrito. Esta operación se realiza, en la etapa de prueba B_{2b} según la relación:

$$AD_V_x > AD_V$$

45 En respuesta negativa a la prueba B_{2b} citada anteriormente, tal y como se representa en la fig. 2b, puede efectuarse una llamada de una etapa de fin de invalidación B_{3b} , permitiendo una operación semejante introducir una seguridad en la operación de invalidación propiamente dicha.

50 Por el contrario, en respuesta positiva a la prueba realizada en la etapa B_{2b} , se realiza una etapa de actualización de la fecha de acción en la etapa B_{4b} , verificando esta operación de actualización la misma relación que la etapa de actualización durante la inscripción de un derecho válido B_{4a} en la fig. 2a.

La etapa B_{4b} se sigue entonces de la etapa C de invalidación propiamente dicha consistente en asignar, a la variable de estado del derecho de acceso inscrito S_V , el valor codificado correspondiente a un derecho invalidado $S_V_x = 0$.

55 En referencia a la fig. 2b, el protocolo objeto de la presente invención puede ponerse en práctica además para la invalidación de un derecho de acceso borrado siempre presente en el módulo de control de acceso, $S_V = 2$. En un caso semejante, consiste, en respuesta negativa a la etapa B_{1b} citada anteriormente, en efectuar la actualización de la etapa B_{4b} y después la invalidación en la etapa C, $S_V = S_V_x = 0$. Al igual que en el caso de la fig. 2a, la etapa B_{4b} puede entonces ponerse en práctica después de una etapa B_{5b} y una etapa B_{6b} análogas a las etapas B_{5a} y respectivamente B_{6a} de la fig. 2a.

60 En las situaciones citadas anteriormente, el protocolo objeto de la invención consiste en efectuar una actualización del derecho de acceso por inscripción de un derecho de acceso cuya fecha de acción corresponde a una fecha de invalidación. A este derecho de acceso inscrito se le asigna una variable de estado correspondiente a un derecho de acceso invalidado.

Las operaciones citadas anteriormente permiten posicionar, inscribir respectivamente, un derecho al estado invalidado para impedir su inscripción posterior por medio de un mensaje cuya fecha de acción será anterior.

ES 2 342 375 T3

A continuación se dará una descripción más detallada de una operación de borrado de un derecho de acceso inscrito, implementación conforme al protocolo objeto de la presente invención, en relación con las fig. 2c y 2d.

En estas condiciones se realiza una operación de borrado de un derecho de acceso inscrito a partir de un mensaje EXM para el cual la variable de asignación de estado $S_V_x = 2$ corresponde a un derecho de acceso borrado.

En estas condiciones, tal y como se representa en la fig. 2c, la operación de borrado se inicia, en un terminal de descifrado T_k , mediante la recepción de un mensaje EXM y se disponen las variables expuestas anteriormente en la descripción, para las operaciones de inscripción o de invalidación, sin embargo con la variable de asignación de estado $S_V_x = 2$.

La operación de borrado se efectúa para un derecho de acceso en el módulo de control de acceso cuya variable de estado corresponde a un derecho válido o a un derecho invalidado.

En estas condiciones, la etapa de recepción del mensaje EXM, B_{0c} , va seguida por una etapa de prueba B_{1c} consistente en verificar la existencia en el módulo de control de acceso de un derecho de acceso inscrito correspondiente. La prueba B_{1c} citada anteriormente es semejante a la prueba B_{1a} o B_{1b} de las fig. 2a o 2b y verifica la misma relación. En respuesta negativa a la prueba de la etapa B_{1c} , se invoca una etapa B_{2c} de fin de borrado. En respuesta positiva a la prueba B_{1c} , esta última va seguida por una etapa B_{3c} de verificación de posterioridad de la variable de fecha de acción del mensaje de gestión AD_V_x , con respecto a la variable de fecha de acción del derecho inscrito AD_V . Esta etapa se realiza por comparación de superioridad según la relación:

$$AD_V_x > AD_V$$

En respuesta negativa a la prueba B_{3c} citada anteriormente, el retorno a la invocación de la etapa de fin de borrado B_{2c} puede realizarse en condiciones semejantes a las de fin de invalidación de un derecho descrito en relación con la fig. 2b.

Por el contrario, en respuesta positiva a la prueba de la etapa B_{3c} , la operación de borrado, según el protocolo objeto de la presente invención, puede consistir en la invocación de una etapa de actualización de la fecha de acción del derecho inscrito, en la etapa B_{4c} , según la relación:

$$AD_V = AD_V_x$$

La etapa de actualización citada anteriormente se sigue entonces de la etapa de borrado propiamente dicha, en la etapa C, para realizar un borrado virtual del derecho de acceso inscrito.

Según una puesta en práctica particularmente ventajosa del protocolo objeto de la presente invención, la etapa de borrado virtual consiste en una atribución, a la variable de estado del derecho de inscrito S_V , de la variable de asignación de estado del mensaje de gestión S_V correspondiente a un derecho de acceso borrado, es decir, $S_V_x = 2$.

La noción de borrado virtual cubre de hecho la noción de mantenimiento de la existencia física del derecho de acceso inscrito en la memoria no volátil del módulo de acceso, siempre que, sin embargo, este derecho se vuelva inutilizable por la sola asignación del valor codificado correspondiente a un derecho de acceso borrado.

Según un modo de puesta en práctica particularmente ventajoso del protocolo objeto de la presente invención, el estado de borrado virtual de un derecho de acceso inscrito puede corresponder a una ausencia de posibilidad de uso total de este derecho, por más que este último se mantenga presente físicamente en la memoria no volátil del módulo de control de acceso que comporta este último. La operación de borrado propiamente dicha, es decir, de borrado físico de todo derecho de acceso inscrito puede realizarse a continuación de manera sistemática, independientemente del control de acceso y del acceso del abonado a las informaciones encriptadas correspondientes al derecho de acceso considerado.

En particular, tal y como se representa en la fig. 2d, el borrado físico del derecho de acceso sometido previamente a un estado de borrado virtual puede ser inmediato o diferido.

Llegado el caso, la ejecución de la etapa de borrado físico puede estar condicionada a un criterio específico, tal como un criterio temporal, y como se describirá de manera más detallada en relación con la fig. 2d.

En referencia a la figura citada anteriormente, se considera un derecho de acceso inscrito en estado de borrado virtual, después de la puesta en práctica del protocolo objeto de la presente invención, conforme al modo de realización ilustrado y descrito anteriormente en la descripción, en relación con la fig. 2c.

En esta situación, se ha recibido un mensaje EXM, con $S_V_x = 2$, y la situación de borrado virtual corresponde a la relación descrita anteriormente en la descripción $S_V = S_V_x = 2$. El estado correspondiente de borrado virtual se representa mediante el estado C_{0d} de la fig. 2d.

ES 2 342 375 T3

La ejecución del borrado físico propiamente dicho del derecho inscrito puede someterse entonces a una prueba tal como una prueba temporal, en la etapa C_{1d} .

La prueba citada anteriormente puede, a título de ejemplo no limitativo, consistir en comparar la variable de fecha de acción del mensaje EXM, es decir, la variable AD_{V_x} , por comparación de superioridad, con la variable de fecha de fin de validez V_D del derecho inscrito.

En respuesta positiva a la prueba C_{1d} , siendo la fecha de acción de borrado posterior a la fecha de validez del derecho inscrito, el borrado físico se realiza de manera inmediata por invocación de una etapa correspondiente C_{3d} .

Por el contrario, en respuesta negativa a la prueba C_{1d} , siendo la fecha de acción de borrado anterior a la fecha de fin de validez V_D del derecho inscrito, una etapa de borrado físico diferida se denomina C_{2d} . El borrado se difiere en tanto que la fecha de acción AD_{V_x} de todos los mensajes de borrado EXM sucesivos sea inferior o igual a la fecha de fin de validez del derecho inscrito. El mantenimiento del borrado físico diferido se simboliza por el retorno a la prueba C_{1d} .

Se comprende que, gracias a la puesta en práctica del borrado diferido citado anteriormente, es posible asegurar una gestión sistemática del borrado físico de los derechos de acceso inscritos siempre que estos últimos, por más que estén siempre presentes físicamente en la tarjeta, sean inutilizables por el abonado cuyo derecho inscrito correspondiente se ha colocado en situación de borrado virtual.

A continuación se dará un ejemplo comparativo de puesta en práctica de borrado o supresión de derecho, conforme a la técnica, respectivamente conforme al protocolo objeto de la presente invención, en la descripción en el caso en que se considera, para un abonado considerado, la ausencia de presencia del módulo de control de acceso, es decir, de la tarjeta atribuida a este último en el terminal de descifrado o decodificador o, llegado el caso, la ausencia de funcionamiento del decodificador durante un periodo de tiempo determinado con respecto a la emisión cíclica de mensajes de gestión, mensajes EMM en el caso de la técnica anterior, mensajes EXM conforme al protocolo objeto de la presente invención.

Se considera así la difusión cíclica de mensajes de gestión de tipo EMM en el caso de los procedimientos de la técnica anterior y de tipo EXM durante la puesta en práctica del protocolo objeto de la presente invención.

Según la tabla 1 relativa al procedimiento de la técnica anterior, se considera la emisión de un ciclo de mensajes de gestión de tipo EMM según un primer ciclo, como el representado en la tabla, siempre que durante las fechas de acción correspondientes, según las casillas de la zona A de la tabla del ciclo 1, el módulo de control de acceso o el terminal de descifrado están fuera de servicio.

(Tabla pasa a página siguiente)

TABLA 1

	Tipo de mensajes	Fecha de la acción	Acción en la tarjeta	
Ciclo 1	.../...		Anterior al 01/12/01	A
	EMM de inscripción R_ID ₁	01/12/01	Derecho inscrito R_ID ₁	
	EMM de supresión R_ID ₁	02/12/01	Derecho borrado R_ID ₁	
	EMM de inscripción R_ID ₂	12/12/01	Derecho inscrito R_ID ₂	
	EMM de inscripción R_ID ₃	13/12/01		
	EMM de inscripción R_ID ₄	12/12/01		
	EMM .../...	.../...		
Ciclo 2	EMM de inscripción R_ID ₅	31/12/01	Derecho inscrito R_ID ₅	
	EMM de supresión R_ID ₅	01/01/02	Derecho borrado R_ID ₅	
	EMM de inscripción R_ID ₆	12/01/02	Derecho inscrito R_ID ₆	
	EMM .../...			
n Ciclo 1	EMM de inscripción R_ID ₁	01/12/01	Derecho inscrito R_ID ₁	B
	EMM de supresión R_ID ₁	02/12/01	Derecho borrado R_ID ₁	
	EMM de inscripción R_ID ₂	12/12/01	Derecho ya inscrito	
	EMM de inscripción R_ID ₃	13/12/01	Derecho inscrito R_ID ₃	
	EMM de inscripción R_ID ₄	12/12/01	Derecho inscrito R_ID ₄	
	EMM .../...			

En la tabla 1 citada anteriormente, se recuerda que la fecha de la acción designa la fecha de emisión del mensaje, pero este mensaje no incluye sin embargo ninguna fecha de acción, al contrario que los mensajes EXM que permiten la puesta en práctica del protocolo objeto de la presente invención.

El ciclo 1 va seguida por un ciclo 2 en fechas diferentes, y después, a continuación, de una pluralidad de ciclos 1, designándose uno de los ciclos mediante n ciclo 1.

Durante la difusión del primer ciclo 1, se realiza toda operación de inscripción de derecho o de supresión de derecho, es decir, de borrado, salvo, naturalmente, en lo que concierne a las casillas de la zona A en las cuales el módulo de control de acceso, es decir, la tarjeta y/o el terminal de descriptado, están fuera de servicio.

Durante la emisión de un ciclo 2, diferente del ciclo 1, en lo que concierne a la variable de identificación de los derechos de acceso inscritos, estando en servicio el módulo de control de acceso y/o el terminal, las operaciones correspondientes se ejecutan de la misma forma.

Por el contrario, durante la repetición del ciclo 1, es decir, en la tabla 1, para las casillas del ciclo denominadas n ciclo 1, aparecen casillas correspondientes a una zona B, indicando esta zona que el derecho difundido R_ID₁ inscrito y borrado sucesivamente no puede establecerse efectivamente tal cual en el módulo de control de acceso, es decir, en la tarjeta, ya que no se ha efectuado ningún control por fecha de acción.

Siempre que el procedimiento de la técnica anterior no permita controlar la no reinscripción de derechos borrados, la tabla 2, relativa a la puesta en práctica del protocolo objeto de la presente invención, en una situación análoga, permite reducir los casos en los que los mensajes de gestión EXM introducen disfunciones en las condiciones citadas posteriormente.

ES 2 342 375 T3

TABLA 2

	Tipo de mensajes	Fecha de la acción	Estado del derecho en la tarjeta	
	.../...			
	EXM de inscripción R_ID ₁	01/12/01	Derecho inscrito	
	EXM de invalidación R_ID ₁	02/12/01	Invalidado	I
	EXM de inscripción R_ID ₂	12/12/01	Derecho inscrito	
	EXM de inscripción R_ID ₃	13/12/01		
	EXM de inscripción R_ID ₄	12/12/01		A
	EXM de invalidación de derecho R_ID ₄	13/12/01		
	EXM .../...	.../...		
	EXM de inscripción R_ID ₅	31/12/01	Derecho inscrito	
	EXM de invalidación de derecho R_ID ₅	01/01/02	Invalidado	I
	EXM de inscripción R_ID ₆	12/01/02	Derecho inscrito	
	EXM .../...			
	EXM de inscripción R_ID ₁	01/12/01	Mensaje ignorado	
	EXM de invalidación R_ID ₁	02/12/01	Mensaje ignorado	i
	EXM de inscripción R_ID ₂	12/12/01	Mensaje ignorado	
	EXM de inscripción R_ID ₃	13/12/01	Derecho inscrito	
	EXM de inscripción R_ID ₄	12/12/01	Derecho inscrito	
	EXM de invalidación de derecho R_ID ₄	13/12/01	Invalidado	I
	EXM .../...	.../...		

En estas condiciones, las reglas de tratamiento en el módulo de control de acceso son las siguientes:

- durante una invalidación, marcado del derecho como invalidado I;
- un derecho invalidado sólo puede reactivarse de manera condicional:
- si la fecha de acción, es decir, la variable de fecha de acción del mensaje EXM es inferior o igual a la fecha de acción del derecho inscrito, la acción del mensaje es ignorada en la tarjeta i;
- si la fecha de la acción del mensaje EXM es superior a la fecha de acción de un derecho inscrito, el derecho inscrito se reactualiza, es decir, se reactualiza efectivamente como invalidado o borrado.

En la tabla 2, al igual que en la tabla 1, la zona A corresponde a un tiempo de parada o de disfunción del módulo de control de acceso y/o del terminal de descryptado para el ciclo 1.

- Las zonas I indican que el derecho inscrito ha sido invalidado gracias al mensaje de invalidación, es decir, S_V = S_V_x = 0;

ES 2 342 375 T3

- las casillas de la zona i hacen referencia a la situación según la cual, si la fecha de acción del mensaje EXM es inferior o igual a la fecha de acción del derecho inscrito e incluso invalidado, la acción correspondiente es ignorada en el módulo de control de acceso.

5

Se constata así la existencia de un tratamiento y de una gestión más flexibles y más fluidos del conjunto de los derechos de acceso inscritos en los módulos de control de acceso.

10

Para la puesta en práctica del protocolo objeto de la presente invención, es necesario disponer, naturalmente, de un terminal de descifrado asociado a un módulo de control de acceso a las informaciones encriptadas transmitidas de un centro de emisión hacia el terminal de descifrado citado anteriormente.

15

Tal y como se representa en la fig. 3a, se indica que el módulo de control de acceso asociado al terminal de descifrado correspondiente comprende, inscrito en memoria de este módulo de control de acceso, al menos un derecho de acceso constituido por un conjunto de variables independientes y de variables relacionadas, incluyendo este conjunto al menos, además de una variable de identificación R_ID del derecho inscrito, una variable de fecha de acción en el derecho de acceso inscrito AD_V y una variable de estado que puede tomar uno de los tres valores codificados mencionados anteriormente en la descripción para representar un derecho de acceso válido, un derecho de acceso invalidado o incluso un derecho de acceso borrado. El módulo de control de acceso puede, además, incluir una

20

De una manera general, se indica que el módulo de control de acceso puede estar constituido por un elemento de software o por un elemento de hardware y, en particular, por una tarjeta virtual para realizar el elemento de software citado anteriormente o por una tarjeta con microprocesador provista del procesador de seguridad, tal y como se ha mencionado anteriormente en la descripción.

25

Cuando el módulo de control de acceso es un elemento de software, éste puede implantarse, por ejemplo, en el terminal de descifrado. En este caso, tal y como se representa en la fig. 3a, el derecho de acceso constituido por el conjunto de las variables independientes y las variables relacionadas citadas anteriormente puede entonces memorizarse en una memoria permanente como, por ejemplo, un disco duro, no representado en los dibujos, y cargarse sistemáticamente en la memoria de trabajo del terminal de descifrado, estando la memoria de trabajo conectada, naturalmente, al procesador de seguridad CPU_S del terminal de descifrado.

30

Cuando, por el contrario, el módulo de control de acceso está constituido por una tarjeta con microprocesador dotada de un procesador de seguridad, tal y como se representa en la fig. 3b, esta tarjeta con microprocesador está provista igualmente de una memoria programable no volátil segura asociada al procesador de seguridad. En tal caso, tal y como se representa en la fig. 3b citada anteriormente, los derechos de acceso constituidos por un conjunto de variables independientes y de variables relacionadas están inscritos en la memoria programable no volátil segura.

35

Se comprende, en particular que, gracias a un enlace por bus hacia los circuitos de entrada/salida denominados I/O de la tarjeta, el intercambio de instrucciones que llegan del terminal de descifrado para asegurar ya sea la inscripción de un derecho de acceso o bien la invalidación de un derecho de acceso, o bien, por el contrario, el borrado de un derecho de acceso en la memoria no volátil programable, puede realizarse mediante los circuitos de entrada/salida I/O citados anteriormente bajo el control del procesador de seguridad CPU_S mencionado anteriormente.

40

Finalmente, en referencia a la misma fig. 3b, y en el caso más particular de un servicio de control de acceso de informaciones encriptadas, acordándose el acceso a estas informaciones a título oneroso, tal como, por ejemplo, en el caso de un servicio de televisión de pago, la noción de derecho de acceso constituido por un conjunto de variables independientes y de variables relacionadas y que define los modos de acceso a las informaciones encriptadas, cubre los monederos electrónicos atribuidos al usuario abonado poseedor del módulo de control de acceso.

50

Por esta razón, en la fig. 3b, se ha representado un monedero electrónico codificado de manera semejante a la de un derecho de acceso AR, pudiendo el monedero electrónico incluir, de la misma manera a título de ejemplo:

55

- una variable de identificación de monedero electrónico llamada Purse Id;
- una variable de fechas de validez V_D;
- una variable de fecha de acción en el monedero electrónico AD_V;
- una variable de estado S_V.

60

Finalmente, puede preverse una variable de unidades de cuenta, denominada Purse Units.

65

Se indica que la variable de identificación de monedero electrónico puede asociarse a una variable relacionada denominada Purse Subld, siendo esta variable, según las convenciones de notación precedentes relativas al derecho de acceso AR, por ejemplo, una variable opcional.

ES 2 342 375 T3

En estas condiciones, se comprende que, para un monedero electrónico dado, referido como Purse Id, es posible definir submonederos, definido cada uno por la variable Purse SubId, para aplicaciones específicas y servicios particulares.

Sucede lo mismo en lo que concierne a la variable de unidades de cuenta Purse Units, a la cual puede asociarse una variable relacionada opcional RE, según las mismas convenciones. La variable relacionada RE puede designar una variable denominada de informe que permite el informe del contenido del monedero electrónico considerado o del saldo acreedor de este último en un monedero electrónico de la misma naturaleza o en el mismo monedero o monedero electrónico que incluye un identificador idéntico.

En estas condiciones, y al igual que en el caso de los derechos de acceso AR, la sintaxis de codificación de los monederos electrónicos, de manera semejante a la de los derechos de acceso AR, es de la forma:

$$PU = \text{Purse Id} [\text{Purse SubId}] V_D AD_V S_V \text{Purse Units} [RE]$$

Documentos indicados en la descripción

En la lista de documentos indicados por el solicitante se ha recogido exclusivamente para información del lector, y no es parte constituyente del documento de patente europeo. Ha sido recopilada con el mayor cuidado; sin embargo, la EPA no asume ninguna responsabilidad por posibles errores u omisiones.

Literatura de ninguna patente citada en la descripción

- D.VAN SSHHONEVELD. Standardization of conditional access systems for digital pay television. *Philips Journal of Research*, 1996, vol. 50, 217-225 [0013]

REIVINDICACIONES

1. Procedimiento de inscripción, de invalidación/borrado de derechos de acceso a informaciones encriptadas transmitidas desde un centro de emisión hacia al menos un terminal de descryptado al que se asocia un módulo de control de acceso dotado de un procesador de seguridad, estando estos derechos de acceso inscritos en dicho módulo de control de acceso, estando dichas informaciones encriptadas sometidas a un control de acceso por emisión periódica de mensajes de control de acceso, portadores de criterios de acceso y de un criptograma de una palabra de control cambiada periódicamente y cifrada por medio de una clave de explotación, y después, en cada procesador de seguridad, condicionado a la verificación del valor verdadero de al menos un derecho de acceso inscrito con respecto a dichos criterios de acceso, por desciframiento del criptograma de la palabra de control a partir de dicha clave de explotación, transmisión al terminal de descryptado de la palabra de control restituida y descryptado de dichas informaciones encriptadas a partir de dicha palabra de control restituida, **caracterizado** porque consiste al menos en:

- constituir todo derecho de acceso inscrito en dicho módulo de control de acceso como un conjunto de variables independientes y de variables relacionadas que incluyen al menos, además de una variable de identificación del derecho de acceso, una variable de fecha de acción en el derecho de acceso inscrito y una variable de estado que puede tomar uno de tres valores codificados como derecho de acceso válido, derecho de acceso invalidado y derecho de acceso borrado;
- transmitir a partir de dicho centro de emisión hacia cada terminal de descryptado y hacia el módulo de control de acceso asociado a este último al menos un mensaje de gestión de derecho de acceso, comportando dicho mensaje al menos, además de una variable de identificación de derecho de acceso inscrito, una variable de fecha de acción y una variable de asignación de estado, correspondiendo el valor codificado a un derecho de acceso válido, un derecho de acceso invalidado o un derecho de acceso borrado; y en recepción de dicho mensaje de gestión de derecho de acceso, al nivel de dicho módulo de control de acceso,
- asignar, al derecho de acceso inscrito correspondiente a la variable de identificación de derecho de acceso de dicho mensaje de gestión de derecho de acceso, dicha fecha de acción, y
- atribuir, a dicha variable de estado de dicho derecho de acceso inscrito correspondiente, dicha variable de asignación de estado correspondiente a un derecho de acceso válido, a un derecho de acceso invalidado o a un derecho de acceso borrado.

2. Procedimiento según la reivindicación 1, **caracterizado** porque, para una operación de inscripción de un derecho de acceso determinado en un módulo de control de acceso, dicha variable de fecha de acción de dicho mensaje de gestión de derecho de acceso corresponde a una fecha de inscripción, y la variable de asignación de estado es un valor codificado correspondiente a un derecho válido, consistiendo la operación de inscripción en inscribir, en dicho módulo de control de acceso, un derecho de acceso determinado cuya fecha de acción es la de dicha fecha de inscripción y cuya variable de estado es la de dicha variable de estado y corresponde a un derecho válido.

3. Procedimiento según la reivindicación 2, **caracterizado** porque, previamente a la operación de inscripción propiamente dicha de dicho derecho de acceso determinado, éste consiste además, al nivel de dicho módulo de control de acceso,

- en verificar la existencia, en dicho módulo de control de acceso, de un derecho de acceso inscrito correspondiente a dicho derecho de acceso determinado y cuya variable de estado corresponde al valor codificado de derecho válido o derecho invalidado, y en respuesta positiva a dicha verificación;
- en verificar el carácter de posterioridad de dicha variable de fecha de acción correspondiente a una fecha de inscripción con respecto a la fecha de acción de dicho derecho de acceso idéntico y en respuesta positiva a dicha verificación de carácter de posterioridad,
- en efectuar una actualización de dicha variable de fecha de acción de dicho derecho de acceso idéntico, a partir de dicha fecha de acción correspondiente a una fecha de inscripción,
- en asignar, a dicha variable de estado de dicho derecho de acceso idéntico, el valor codificado correspondiente a un derecho válido, lo que permite validar dicho derecho de acceso inscrito.

4. Procedimiento según la reivindicación 2 ó 3, **caracterizado** porque, en respuesta negativa a dicha verificación de existencia de un derecho de acceso idéntico, éste consiste además en efectuar una actualización en primera inscripción de este derecho de acceso, cuya fecha de acción corresponde a la fecha de inscripción.

5. Procedimiento según la reivindicación 1, **caracterizado** porque, para una operación de invalidación de un derecho de acceso inscrito en un módulo de control de acceso, dicha variable de fecha de acción de dicho mensaje de gestión de derecho de acceso corresponde a una fecha de invalidación y la variable de asignación de estado es un va-

lor codificado correspondiente a un derecho invalidado, consistiendo la operación de invalidación en asignar, a dicha variable de estado de dicho derecho de acceso inscrito, dicho valor codificado correspondiente a un derecho invalidado y en actualizar dicha fecha de acción de dicho derecho de acceso inscrito a partir de dicha fecha de invalidación.

6. Procedimiento según la reivindicación 5, **caracterizado** porque, previamente a la operación de invalidación propiamente dicha, éste consiste:

- en verificar la existencia, al nivel de dicho módulo de control de acceso, de un derecho de acceso inscrito correspondiente a dicho derecho de acceso de dicho mensaje de gestión;
- en verificar el carácter de posterioridad de dicha variable de fecha de acción correspondiente a una fecha de invalidación con respecto a dicha variable de fecha de acción de dicho derecho inscrito.

7. Procedimiento según una de las reivindicaciones precedentes, **caracterizado** porque, para toda variable de asignación de estado del mensaje de gestión correspondiente a un derecho de acceso borrado y para todo derecho de acceso inscrito en el módulo de control de acceso cuya variable de estado corresponde a un derecho válido o a un derecho invalidado, éste consiste al menos:

- en una actualización de la fecha de acción de dicho derecho inscrito;
- en una atribución, a dicha variable de estado de dicho derecho de acceso inscrito, de dicha variable de asignación de estado del mensaje de gestión correspondiente a un derecho de acceso borrado, constituyendo dicha operación de atribución, para dicho derecho de acceso inscrito, una operación de borrado virtual.

8. Procedimiento según la reivindicación 7, **caracterizado** porque las etapas de actualización y de borrado virtual de dicho derecho de acceso inscrito están precedidas por una etapa de verificación de la existencia, en dicho módulo de control de acceso, de un derecho de acceso inscrito correspondiente a dicho derecho de acceso de dicho mensaje de gestión, y por una etapa de verificación de posterioridad de dicha variable de fecha de acción de dicho mensaje de gestión con respecto a dicha variable de fecha de acción de dicho derecho de acceso inscrito.

9. Procedimiento según una de las reivindicaciones 7 u 8, **caracterizado** porque dicha operación de borrado virtual va seguida por una operación de borrado físico de dicho derecho de acceso.

10. Procedimiento según la reivindicación 9, **caracterizado** porque dicha operación de borrado físico es inmediata o diferida.

11. Procedimiento según una de las reivindicaciones 2 ó 3, **caracterizado** porque, para un derecho de acceso inscrito cuya variable de asignación de estado corresponde a un derecho de acceso borrado, éste consiste además en efectuar una actualización en primera inscripción de este derecho de acceso, a dicho derecho de acceso, siendo asignada una variable de estado correspondiente a un derecho válido y cuya fecha de acción corresponde a la fecha de inscripción.

12. Procedimiento según una de las reivindicaciones 5 ó 6, **caracterizado** porque, para un derecho de acceso inscrito cuya variable de asignación de estado corresponde a un derecho de acceso borrado, éste consiste además en efectuar una actualización en primera inscripción de este derecho de acceso, a dicho derecho de acceso, estando asignada una variable de estado correspondiente a un derecho invalidado y cuya fecha de acción corresponde a la fecha de inscripción.

13. Procedimiento según una de las reivindicaciones 5 ó 6, **caracterizado** porque, en respuesta negativa a dicha verificación de existencia de un derecho de acceso correspondiente, éste consiste además en efectuar una actualización en primera inscripción de este derecho de acceso, cuya fecha de acción corresponde a una fecha de invalidación, a dicho derecho de acceso, estando asignada una variable de estado correspondiente a un derecho invalidado.

14. Módulo de control de acceso destinado a la puesta en práctica del procedimiento de una cualquiera de las reivindicaciones precedentes, estando dotado este módulo de control de acceso de un procesador de seguridad en el que están inscritos los derechos de acceso a las informaciones encriptadas, siendo el procesador de seguridad apto para descifrar el criptograma de la palabra de control a partir de la clave de explotación, y siendo el módulo de control de acceso apto para transmitir al terminal de descifrado la palabra de control restituida para que las informaciones encriptadas a partir de la palabra de control restituida puedan descifrarse, **caracterizado** porque comprende, inscrito en memoria de este módulo de control de acceso, al menos un derecho de acceso constituido por un conjunto de variables independientes y de variables relacionadas, que comprenden al menos, además de una variable de identificación del derecho de acceso inscrito y una variable de fechas de validez, una variable de fecha de acción en el derecho de acceso inscrito y una variable de estado que puede tomar uno de tres valores codificados, derecho de acceso válido, derecho de acceso invalidado y derecho de acceso borrado.

ES 2 342 375 T3

15. Módulo de control de acceso según la reivindicación 14, **caracterizado** porque dicho módulo de control de acceso está constituido por una tarjeta de microprocesador dotada de un procesador de seguridad y de una memoria programable no volátil asegurada, estando dicho al menos un derecho de acceso inscrito en dicha memoria programable no volátil asegurada.

16. Módulo de control de acceso según la reivindicación 14 ó 15, **caracterizado** porque, para un control de acceso a las informaciones encriptadas de un servicio de televisión de pago, dichos derechos de acceso cubren dichos derechos de acceso que definen los modos de acceso a dichas informaciones encriptadas y a los monederos electrónicos atribuidos al usuario abonado, poseedor de dicho módulo de control de acceso.

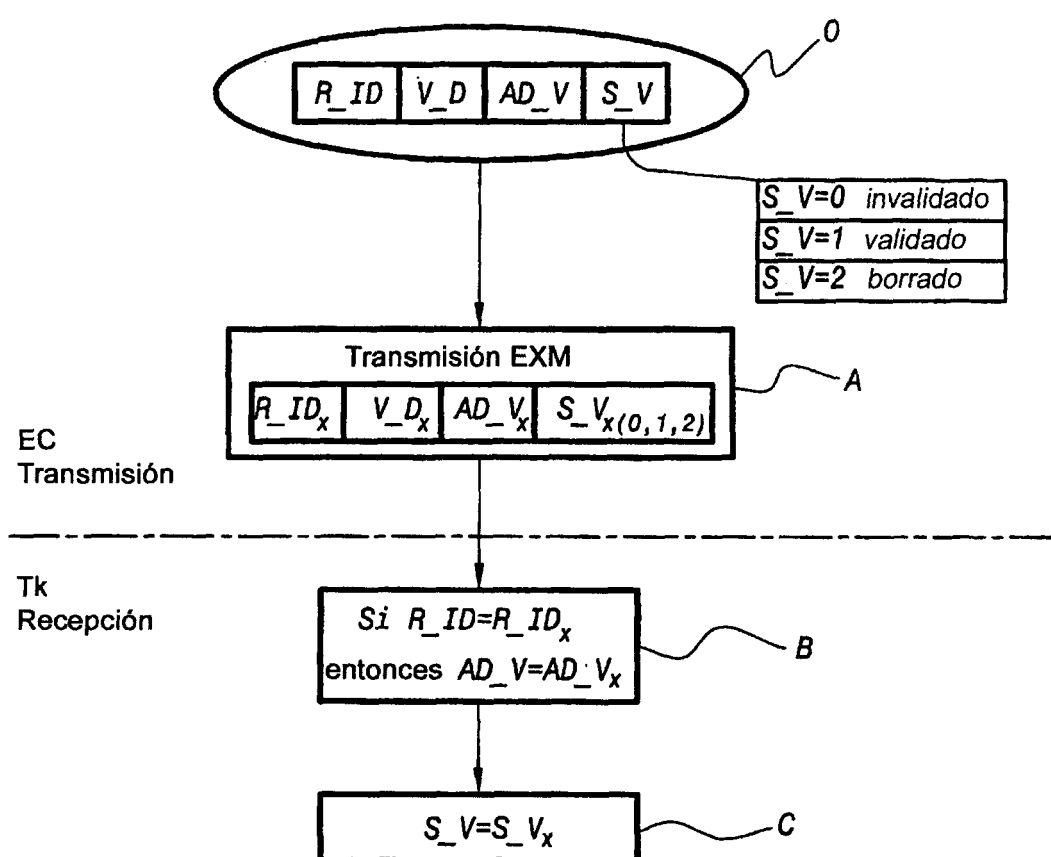


FIG.1

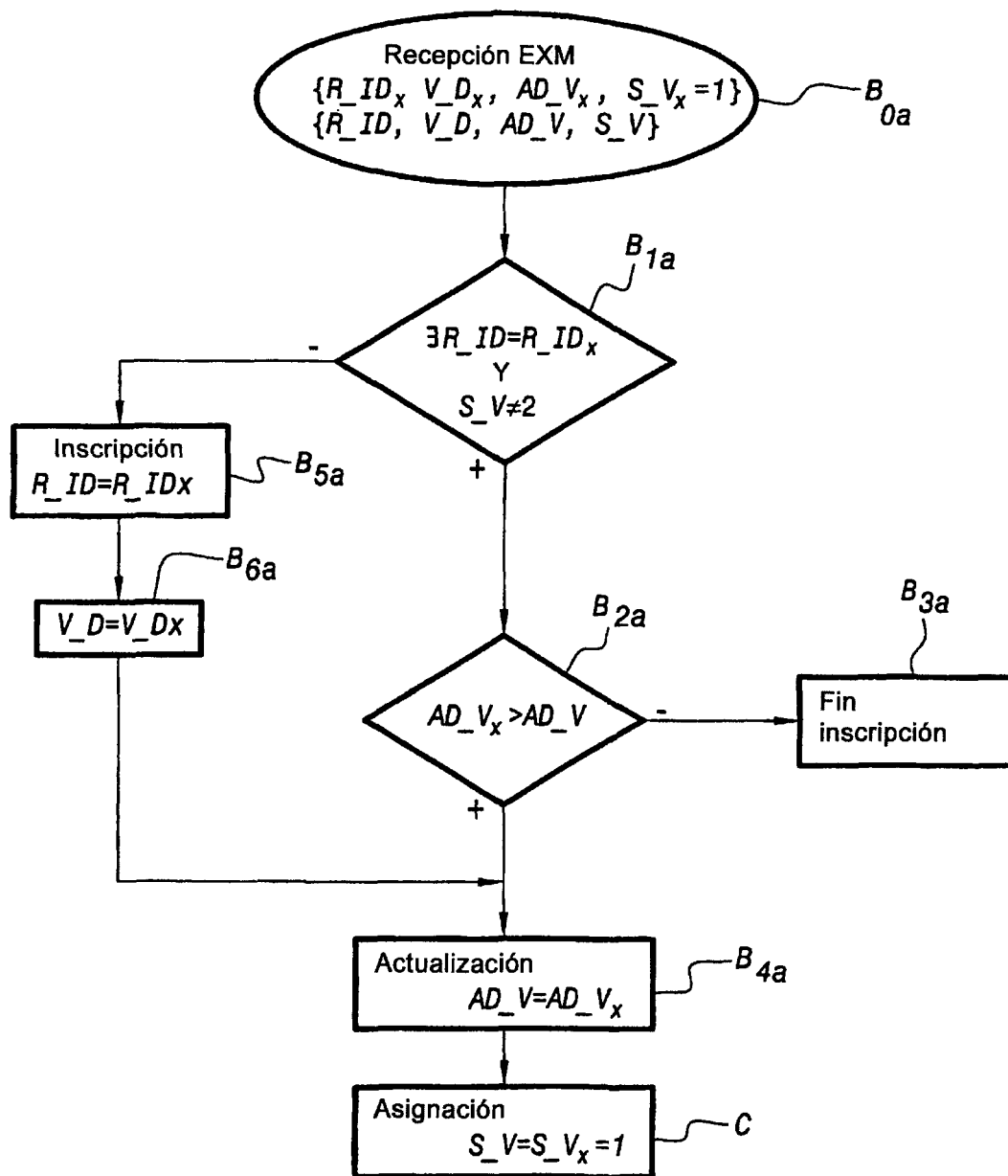


FIG.2a

Inscripción de un derecho válido

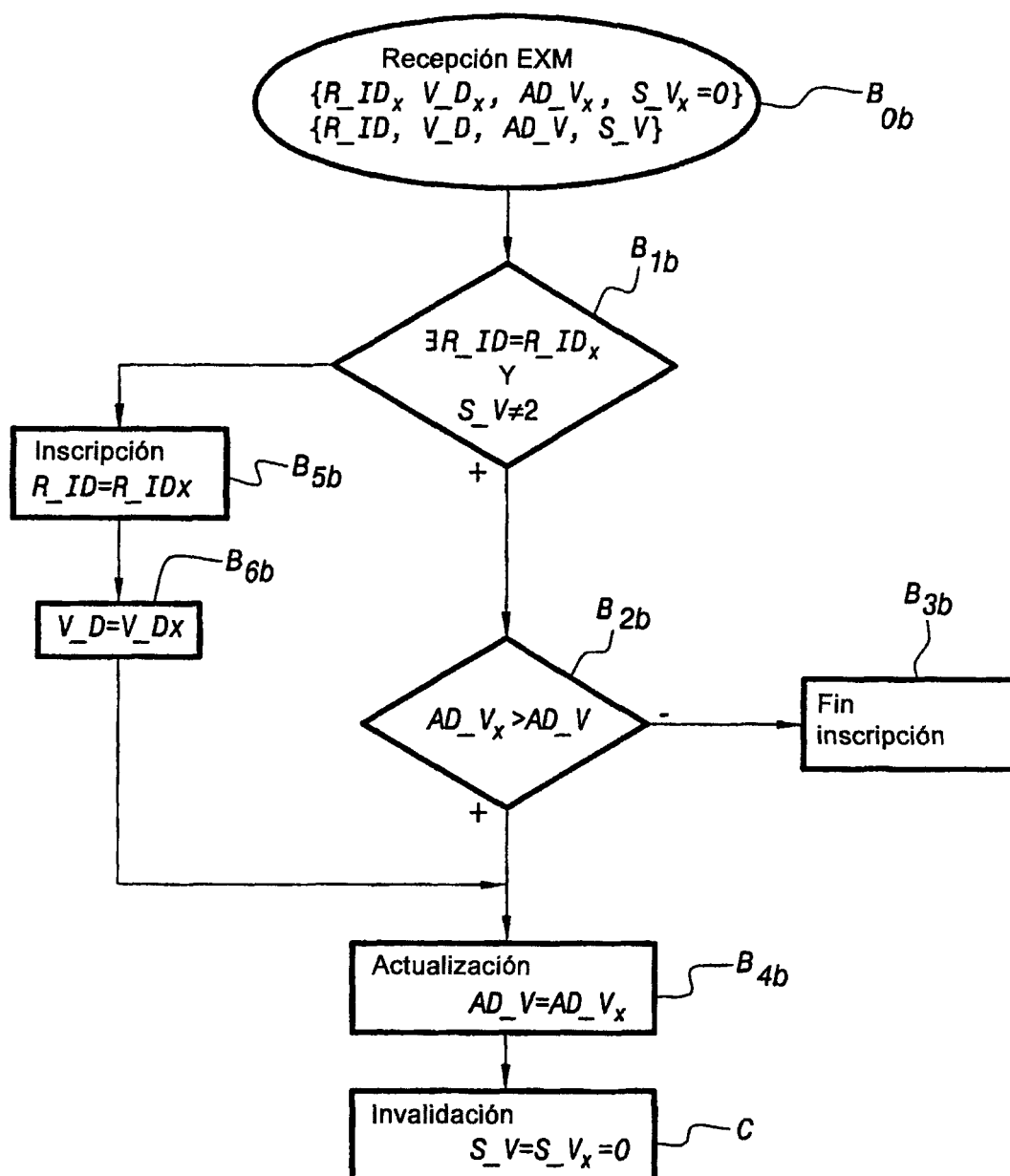


FIG.2b

Invalidación de un derecho

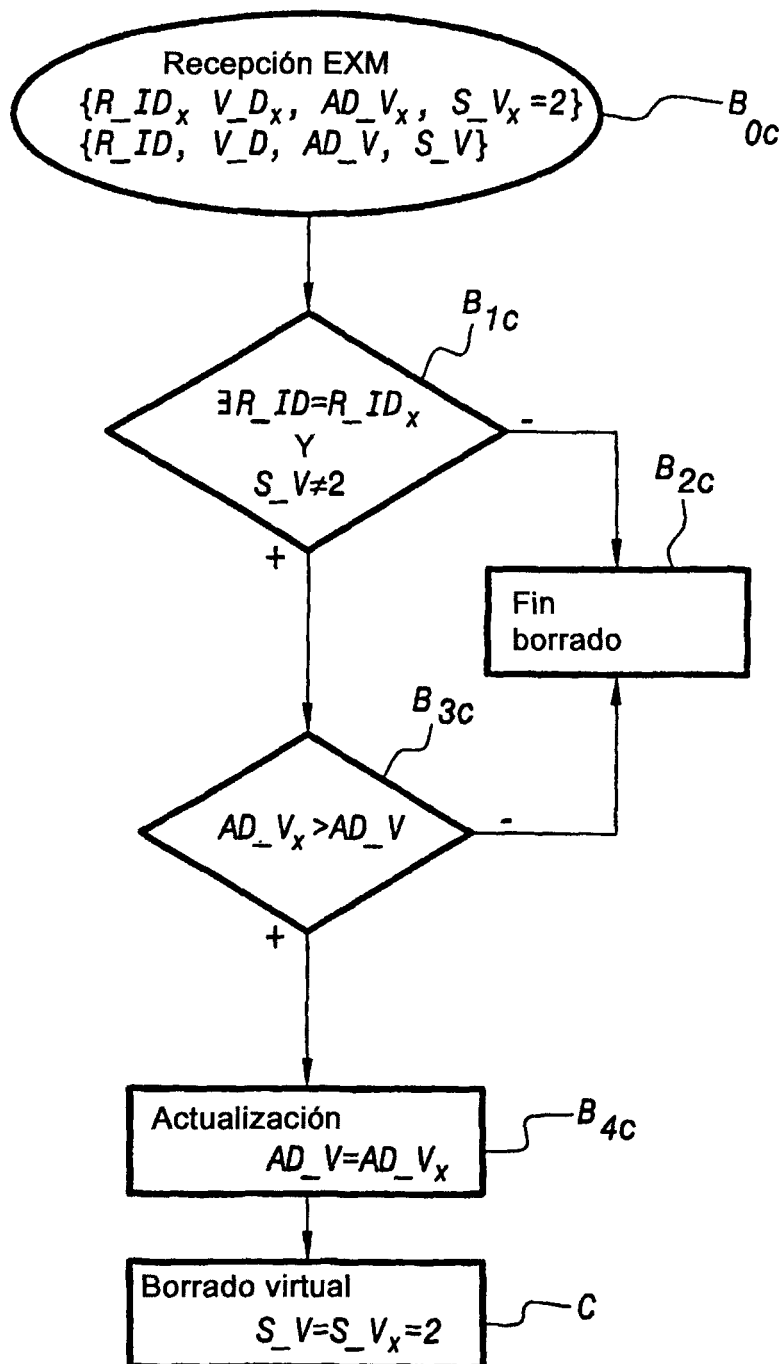


FIG.2c

Borrado virtual de un derecho

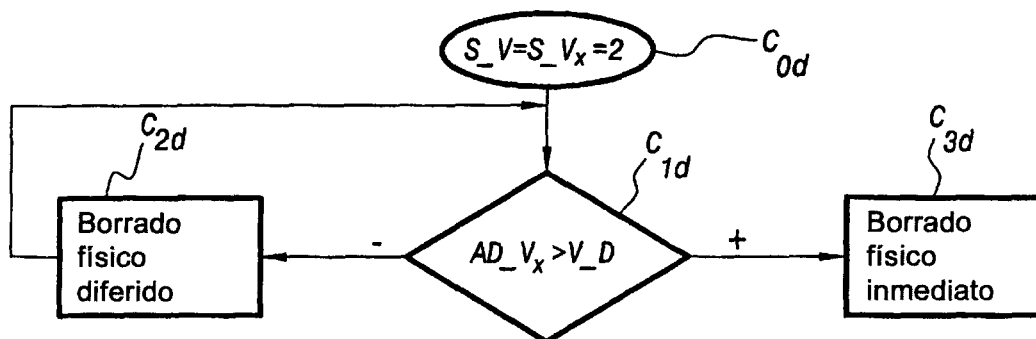


FIG. 2d

Borrado físico

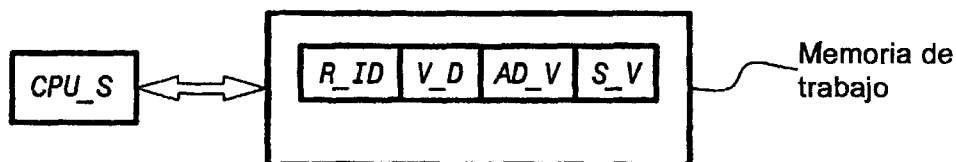


FIG. 3a

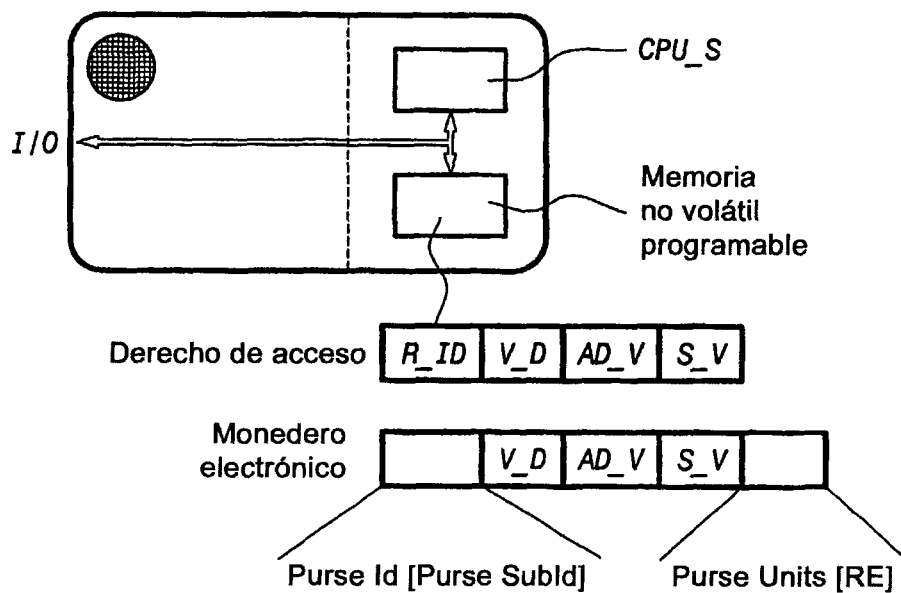


FIG. 3b