(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 633 645**

(51) Int. CI.:

H04N 7/173 (2011.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **13.03.2007 PCT/EP2007/052319**

(87) Fecha y número de publicación internacional: **20.09.2007 WO07104749**

(96) Fecha de presentación y número de la solicitud europea: **13.03.2007 E 07726825 (8)**

(97) Fecha y número de publicación de la concesión europea: **03.05.2017 EP 1994750**

(54) Título: **Método de validación de acceso a un producto mediante un módulo de seguridad**

(30) Prioridad:

13.03.2006 EP 06290423

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
22.09.2017

(73) Titular/es:

NAGRAVISION S.A. (100.0%)
22-24, ROUTE DE GENEVE
1022 CHESEAUX-SUR-LAUSANNE, CH

(72) Inventor/es:

PARISOT, LAURENCE

(74) Agente/Representante:

TOMAS GIL, Tesifonte Enrique

DESCRIPCIÓN

Método de validación de acceso a un producto mediante un módulo de seguridad

[0001] La presente invención concierne el campo de la televisión digital de pago donde de los usuarios adquieren derechos de consumo de productos distribuidos a cambio de un pago. Este último se debita de un crédito almacenado en un módulo de seguridad asociado a una unidad de usuario o un descodificador.

Antecedentes de la técnica

[0002] La función de un módulo de seguridad es controlar el acceso a un flujo que transporta datos digitales encriptados puestos a disposición de usuarios por un servidor de difusión. En este caso, en el área de la televisión de pago, un descodificador permite acceder y descodificar el flujo de datos audio/vídeo encriptados que se distribuye en función de los derechos registrados en el módulo de seguridad asociado a dicho descodificador.

[0003] Un módulo de seguridad se presenta generalmente bajo la forma de un módulo electrónico protegido y conocido inviolable como por ejemplo una tarjeta con microprocesador desmontable insertada en un lector apropiado que la conecta al descodificador.

[0004] Este módulo de seguridad, equipado con interfaces de comunicación, recibe de un centro de gestión mensajes destinados a gestionar los derechos de acceso a los datos difundidos. Estos mensajes se llaman mensajes de gestión de autorización EMM (Entitlement Administration Message).

[0005] El documento WO03/085959 describe un sistema que comprende un centro de gestión que transmite un flujo de datos encriptados a través de contraseñas de control incluidas en mensajes de control (ECM). El flujo de datos se destina a al menos una unidad de usuario vinculada a un módulo de seguridad identificado por una única dirección. Este módulo contiene un crédito que disminuye según la compra de productos o del consumo del flujo de datos. Para recargar el crédito, el usuario comunica al centro de gestión un identificador de usuario representativo de la única dirección del módulo de seguridad y un código de valor que representa el importe de débito. El centro de gestión procesa y verifica el código de valor antes de transmitir al módulo de seguridad un mensaje de gestión (EMM) encriptado que permita recargar el crédito.

[0006] Cuando hay suficiente crédito en el módulo de seguridad son posibles dos modos de compra, a saber:
- compra de modo local: el usuario decide utilizar todo o una parte de su crédito para comprar un producto. Así, se crea un nuevo derecho en el módulo de seguridad para la recepción de dicho producto después de la disminución del crédito.
- compra a través del centro de gestión: el usuario solicita al centro de gestión la compra de un producto. El centro de gestión envía entonces un mensaje de gestión (EMM) encriptado que contiene el derecho de acceso a dicho producto así como el importe a disminuir del crédito del módulo de seguridad.

[0007] La compra se efectúa en ambos casos mediante el procesamiento de mensajes que contienen un derecho para un producto así como el coste correspondiente. Si hay suficiente crédito disponible, el módulo de seguridad procesa el mensaje, es decir, disminuye el crédito y valida el derecho. Este libera el acceso a un producto comercializado en el momento de su recepción.

[0008] En el caso de que el crédito almacenado en el módulo de seguridad fuera insuficiente, el mensaje de gestión EMM recibido se rechazaría y el acceso al producto solicitado no sería posible.
También puede producirse el mismo efecto cuando la unidad del usuario está fuera de servicio, lo que causa que el derecho que se solicita no se pueda validar. El sistema de control de acceso y el centro de gestión, de este modo, no tienen ninguna información sobre el uso real del crédito, lo que representa un inconveniente cuando se trata de establecer cuentas para los proveedores de los productos.

[0009] Como las unidades de usuarios no disponen de una vía de retorno directo hacia el sistema de control de acceso, los índices de consumo real de los productos respecto a los mensajes enviados no se pueden determinar. En efecto, al ser los mensajes emitidos más numerosos que aquellos que efectivamente se procesan localmente para liberar el acceso al producto, el centro de gestión se arriesga a pagar a los proveedores excedentes de derechos y/o de productos que los usuarios nunca han consumido ni pagado.

[0010] Cuando se efectúa una compra a través del centro de gestión, el usuario transmite una solicitud que comprende un identificador de usuario del módulo de seguridad y un código relativo al producto o al servicio seleccionado. En el caso de que esta transmisión se efectúe a través de un canal de retorno independiente al canal de recepción de los datos difundidos, como por ejemplo que la solicitud se comunique por teléfono o por mensaje corto SMS, no se podrá efectuar una verificación de concordancia entre el número de usuario del módulo de seguridad y el usuario real. En efecto, sería posible generar códigos de servicios y de productos con

identificadores de usuario de módulo de seguridad con ayuda de un software adecuado por ejemplo, y transmitirlos al centro de gestión. Este último analiza estas solicitudes, acepta aquellas cuyo identificador de usuario de módulo de seguridad se reconoce en la base de datos del centro para emitir los mensajes de administración EMM destinados a las unidades relativas a los identificadores de usuario de módulo de seguridad reconocidos. En el momento de la recepción de estos mensajes EMM, los módulos de seguridad correspondientes a los identificadores de usuario de módulo reconocidos verán sus créditos debitados sin que lo sepan los usuarios de las unidades en cuestión. Un error en la introducción del código por parte del usuario puede acabar igualmente con la transmisión de un mensaje EMM causando un débito inoportuno de un crédito de una unidad de otra persona. La probabilidad de tal débito se incrementa proporcionalmente al número de unidades en servicio en la red.

[0011] El documento US6810525 describe un método y un sistema de compra impulsiva de servicios a través de una red de comunicación. Una solicitud de compra de un servicio se transmite por un terminal de abonado a un centro de control de acceso que genera un mensaje encriptado que incluye un identificador de servicio y derechos asociados. El terminal recibe este mensaje acompañado del coste del servicio seleccionado y verifica si el crédito disponible es suficiente. En caso de éxito de la verificación, un testigo de seguridad se genera por una aplicación del terminal. Este testigo se envía a un servidor de la red para determinar el estado de los derechos del abonado antes del procesamiento de la solicitud de compra por el centro de control de acceso. Este sistema de compra de servicios se aplica a una configuración en red bidireccional en la cual los terminales de abonados se conectan sin interrupción al centro de control de acceso y al servidor de verificación de los testigos. Constituye una solución al problema de cargos indeseados de otros usuarios porque utiliza una transmisión de punto a punto de los ficheros de verificación utilizando preferiblemente una vía de retorno dependiente del terminal. En cambio, el método puede ejecutarse difícilmente de manera automática en un sistema de difusión con una vía de retorno independiente del terminal que se utiliza para el envío de solicitudes únicas. Una ejecución manual implicaría la transmisión por el usuario de dos mensajes: la solicitud de compra y el testigo generado por el terminal. Este método se volvería así de repetitivo y molesto para la compra espontánea y rápida de servicios disponibles en línea.

[0012] El documento EP1398966 describe un sistema de transacción efectuado por un usuario de un receptor sin canal de retorno. El sistema comprende un centro de difusión (*head-end*), una red de comunicación y un receptor equipado con un medio de visualización apto para recibir datos digitales transmitidos por el centro de difusión a través de la red de comunicación. El receptor comprende un módulo de seguridad configurado para visualizar un primer código único de identificación del módulo destinado a crear un testigo de transacción. También se visualiza un segundo código que identifica un servicio o un producto solicitado, este código está incluido en los datos del producto comercializado. En el momento de la compra, el usuario selecciona un producto del que se transmite el código de identificación y el precio conjuntamente al código único del módulo de seguridad (testigo de transacción) al centro de difusión. Esta transmisión se efectúa por una vía independiente al receptor, como teléfono vocal, mensaje corto SMS u otro. El centro de difusión decodifica el testigo y libera el producto después de la identificación en una base de datos del identificador del módulo de seguridad que se extrae del testigo.

[0013] Este sistema se expone al problema de débitos indeseados de otros usuarios por la transmisión de códigos de identificaciones que pueden reconocerse por el centro de difusión y corresponde a los módulos de seguridad en servicio. Como se trata de una transmisión de datos en modo difusión, los mensajes de administración que permiten liberar el visionado de los productos y debitar un crédito a un receptor dado se difunden a todos los receptores de la red. La encriptación de los ficheros mencionada en el documento EP1398966 puede constituir una solución a este problema. Sin embargo, las claves de encriptación e identificadores de usuario de módulos de seguridad pueden ser determinados por terceros malintencionados que, de este modo pueden, generar testigos de manera sistemática para provocar débitos en un número más o menos elevado de receptores.

[0014] El documento US2006/015580A1 describe un sistema que comprende un servidor multimedia, una base de datos de perfiles de usuarios y un servidor de aplicación conectado a una o a varias redes de comunicación. Con la recepción de una solicitud de visionado de un contenido transmitido por una unidad de usuario, el servidor de aplicación solicita la base de datos de perfil de usuario para determinar el propietario de la unidad de usuario y sus derechos de acceso al contenido basándose en un identificador de la unidad de usuario transmitido en la solicitud. El servidor de aplicación solicita el servidor multimedia para difundir un flujo de formato apropiado que transporta el contenido requerido para el visionado.

Breve descripción de la invención

[0015] El objetivo de la presente invención es paliar los inconvenientes destacados anteriormente para permitir asegurar al centro de gestión un mejor control de los derechos que se les proporcionan a los usuarios por medio de mensajes de administración. En efecto, el centro de gestión transmite los mensajes únicamente cuando el crédito almacenado en el módulo de seguridad de la unidad de usuario es suficiente.

[0016] Otro objetivo es proporcionar un bloqueo contra los débitos abusivos de los créditos provocados por la transmisión de solicitudes ficticias que contienen identificadores de usuario de módulos de seguridad reconocidos por el centro de gestión.

[0017] Este objetivo se alcanza por un método de validación de acceso a un producto por un módulo de seguridad asociado a una unidad de usuario conectada, de manera unidireccional, a un sistema de control de acceso que transmite mensajes de gestión destinados a dicho módulo de seguridad, dichos mensajes se generan por el sistema de control de acceso seguido de la recepción de una solicitud de un derecho de acceso a un producto que consiste en datos digitales emitidos, dicho método comprende las etapas siguientes:

- compra de un producto propuesto por la unidad de usuario y verificación, por el módulo de seguridad, de que el débito asociado al producto está cubierto por un crédito restante,

- en caso afirmativo, determinación de un código representativo del producto comprado,

- visualización de dicho código sobre un órgano de visualización asociada a la unidad de usuario,

- transmisión al centro de gestión, a través de un canal independiente de la unidad de usuario, de una solicitud que comprende al menos dicho código y un identificador de usuario representativo del identificador de usuario del módulo de seguridad,

- verificación por el sistema de control de acceso de la validez del código y del identificador de usuario del módulo de seguridad, transmisión de un mensaje de confirmación de derecho destinado a la unidad de usuario asociada a dicho módulo de seguridad,

caracterizado por el hecho de que, en el momento de la compra del producto, un derecho temporal se inscribe en el módulo de seguridad cuando el crédito restante es igual o superior al importe asociado a dicho producto, dicho derecho temporal se reemplaza por un derecho definitivo mediante el mensaje de confirmación de derecho recibido del centro de gestión, dicho derecho definitivo autoriza el acceso al producto comprado cargando el importe asociado a dicho producto.

[0018] La solución consiste en probar al sistema de control de acceso que el módulo de seguridad es efectivamente apto para crear un derecho para la adquisición de un producto seleccionado. En el momento de la compra del producto, el importe asociado a dicho producto se compara con un crédito restante en el módulo de seguridad. Cuando el crédito restante es superior o igual al importe asociado al producto, un derecho temporal se almacena en el módulo de seguridad. Un código que identifica este derecho propio al producto se asocia al número único que identifica el módulo de seguridad después de que se trasmita al centro de gestión en forma de solicitud de derecho. Al recibir la solicitud, el sistema de control de acceso genera un mensaje de confirmación de derecho que comprende el derecho definitivo y el código identificador del usuario como condición de acceso al derecho definitivo. El módulo de seguridad recibe este mensaje de confirmación y reemplaza el derecho temporal por el derecho definitivo del mensaje solamente si el código identificador del usuario corresponde al derecho temporal. De este modo, el acceso al producto está autorizado. En el caso contrario de que un identificador de usuario de derecho definitivo sea diferente o no esté incluido en los derechos temporales, el mensaje de gestión se rechaza y el acceso al producto se rechaza por falta de un derecho válido.

[0019] La ventaja de este método es que el mensaje de confirmación se genera y transmite por el sistema de control de acceso solamente si la verificación del crédito del módulo de seguridad fue capaz de efectuarse con éxito. Dicho de otro modo, en caso de que el crédito inicial sea insuficiente con respecto a este exigido por el producto, no se podrá generar una solicitud al centro de gestión.

[0020] El centro de gestión y el sistema de control de acceso son en general dos entidades separadas. La primera consiste en una interfaz con el usuario que gestiona las solicitudes de derechos, mientras que la segunda genera los mensajes de gestión que van destinados a las unidades de usuarios según las solicitudes recibidas de la primera entidad. En ciertas configuraciones estas dos entidades pueden reagruparse en un sistema de gestión global.

[0021] Este método resuelve el problema de débitos indeseados de otros usuarios porque el derecho definitivo de acceso al producto comprado solo se atribuye a la unidad cuyo módulo de seguridad contiene el derecho temporal correspondiente al producto seleccionado. Las unidades que no poseen este derecho o que poseen otro derecho que correponda a un módulo de seguridad y/o a un producto diferente no se verán afectadas por el mensaje de confirmación de derecho. De este modo, para que un crédito se cargue definitivamente se necesita la condición complementaria de la presencia del derecho temporal correspondiente a un producto y a un módulo de seguridad dado.

Breve descripción de las figuras

[0022] La invención se comprenderá mejor gracias a la descripción detallada que va a continuación y que hace referencia a las figuras adjuntas que se presentan a modo de ejemplos no limitativos.

- La figura 1 ilustra un esquema funcional de un sistema que lleva a cabo una primera variante del método en la que una solicitud de un derecho de acceso dirigido al centro de gestión comprende un código de compra propio al producto comprado.

- La figura 2 ilustra un esquema funcional de un sistema que lleva a cabo una segunda variante del método en el que una solicitud de un derecho de acceso dirigida al centro de gestión comprende un código de compra que se calcula a partir de los identificadores de usuario del módulo de seguridad y del producto.

Descripción detallada de la invención

[0023] En la primera variante del método esquematizado por la figura 1, un producto (P1) es seleccionado por el usuario en una lista que se muestra en una pantalla de televisión, por ejemplo. La compra del producto pone en marcha un proceso de verificación de un crédito almacenado en el módulo de seguridad (SM) asociado a la unidad de usuario (STB) o descodificador, este crédito debe ser superior o igual al coste del producto (P1) seleccionado. En una variante y particularmente en el caso de compras simultáneas de varios productos, las importes de los costes correspondientes se pueden memorizar en un registro de créditos comprometidos, el crédito restante se carga provisionalmente. Este proceso corresponde a una compra provisional de productos que se validarán a continuación por el sistema de control de acceso (CAS).

[0024] Un derecho temporal (D1t) se inscribe en el módulo de seguridad (SM) cuando el importe del producto (P1) corresponde a una débito inferior o igual al crédito restante en el módulo (SM). Un código (CP1) propio al producto (P1) comprado se genera a partir del derecho temporal (D1t), o se extrae de la descripción del producto (P1). Según un ejemplo de configuración, este código se puede memorizar por el módulo de seguridad (SM) y se asocia al derecho temporal (D1t) cuando se ha efectuado el débito.

[0025] Una aplicación instalada en el descodificador (STB) permite visualizar este código al usuario, por ejemplo en una pantalla de televisión o en un monitor gráfico separado. Para confirmar la compra, el usuario transmite este código (CP1) al centro de gestión (CG) con el identificador de usuario de su módulo de seguridad (ID_{SM}).

[0026] Este mensaje RQ(ID_{SM}, CP1) se transmite a un centro de gestión (CG) a través de un canal de comunicación habitualmente independiente al descodificador (STB), por ejemplo a través de la red telefónica fija o móvil, Internet u otro canal de transmisión.

[0027] La solicitud RQ(ID_{SM}, CP1) se puede transmitir bien en un mensaje corto SMS, por medio de un servidor vocal, por correo electrónico o bien en algún otro soporte aceptado por el centro de gestión (CG).

[0028] Según un ejemplo de realización, el descodificador transmite la solicitud a un teléfono móvil a través de un enlace inalámbrico de tipo Bluetooth o infrarrojo IrDA (Infrared Data Association). Un mensaje corto (SMS) se crea a continuación a partir de los datos recibidos y se transmiten al centro de gestión a través de la red móvil.

[0029] Según otro ejemplo, el descodificador está equipado con una conexión temporal con el centro de gestión que se establece solamente para la transmisión de la solicitud.

[0030] El centro de gestión (CG) proporciona los parámetros de la solicitud al sistema de control de acceso (CAS), que verifica antes de todo la conformidad del identificador (ID_{SM}) del módulo de seguridad así como del código producido (CP1). Un resultado positivo de la verificación autoriza la generación de un mensaje de confirmación (CEMM) que contiene el identificador de usuario del derecho definitivo (D1).

[0031] El módulo de seguridad (SM) recibe el mensaje (CEMM) mediante el descodificador (STB) y reemplaza el derecho temporal (D1t) por el derecho definitivo (D1) si el derecho temporal (D1t) estaba almacenado de forma efectiva en el módulo de seguridad (SM). Así la compra previa efectuada anteriormente se valida autorizando el acceso al producto (P1).

[0032] Con el objetivo de la verificación, el mensaje de confirmación comprende además un código de producto (CP1') y el derecho definitivo (D1) reemplaza el derecho temporal (D1t) solamente si el código del producto (CP1') corresponde al producto (P1) comprado previamente. En la variante donde el módulo de seguridad memoriza el código de producto (CP1), el código (CP1') devuelto por el mensaje de confirmación (CEMM) debe ser idéntico al código (CP1) almacenado.

[0033] La seguridad de esta primera variante de este método puede ponerse en duda por un ataque del sistema que consiste en la transmisión repetida de solicitudes RQ(ID_{SM}, CP1) con identificadores de usuario (IDSM) de módulos de seguridad (SM) válidos acompañados cada uno de un código de producto (CP1) igualmente válido. Estas solicitudes corren el riesgo de sobrecargar el sistema de control de acceso mediante el envío de mensajes de confirmación (CEMM) que nunca se validarán. Además, las estadísticas y el recuento de los productos consumidos destinados a los proveedores estarán falseados en gran medida. En efecto, el sistema de control de acceso (CAS) transmite un número importante de mensajes (CEMM) inútiles sin necesariamente autorizar un acceso a un producto (P1). A pesar de un identificador de usuario de módulo de seguridad (IDSM) válido, el derecho definitivo (D1) puede ser invalidado al no corresponder a ningún derecho temporal (D1t) y al causar el rechazo, por la unidad (STB) que lo recibe, del mensaje de confirmación (CEMM).

[0034] El bloqueo a este ataque consiste, por una parte, en el cálculo por el módulo de seguridad (SM) del identificador de usuario (ID_{D1t}) del derecho temporal a partir del identificador de usuario (ID_{P1}) del producto (P1) comprado y el del módulo de seguridad y, por otra parte, en encriptar este identificador del derecho temporal (IDD1t) con una clave personal (Kp) de la unidad de usuario (STB). El criptograma que se obtiene de este modo forma un código de compra (CA_{P1}).

[0035] La solicitud RQ(ID_{SM}, CAP1; ID_{P1}) de derecho al centro de gestión (CG) comprende entonces el identificador de usuario del módulo de seguridad (ID_{SM}), el código de compra (CA_{P1}) y el identificador de usuario del producto comprado (ID_{P1}). Con la recepción de la solicitud RQ(ID_{SM}, CA_{P1}; ID_{P1}), el sistema de control de acceso (CAS) recalcula el código de compra (CA_{P1}) conociendo la clave personal (Kp) de la unidad de usuario, el identificador de usuario del producto (ID_{P1}) y el identificador de usuario del módulo de seguridad (ID_{SM}). Así puede determinar si el código de compra (CA_{P1}) recibido es válido antes de preparar el mensaje de confirmación (CEMM) en respuesta a la solicitud. En caso de éxito de la comparación, el sistema de control de acceso (CAS) transmite el mensaje (CEMM) condicional que contiene el derecho definitivo (D1) que autoriza el acceso al producto (P1) solamente a la unidad (STB) identificada por el módulo de seguridad de identificador de usuario (ID_{SM}).

[0036] Esta variante del método presenta la ventaja de hacer el ataque sistemático descrito anteriormente mucho más difícil debido a que el código de compra (CA_{P1}) depende a la vez de los identificadores de usuario del módulo de seguridad (ID_{SM}) y del producto (ID_{P1}) en lugar de solo el identificador del producto (ID_{P1}) como en la variante precedente. El código de compra (CA_{P1}) está además encriptado con una clave personal (Kp) guardada en secreto en el módulo de seguridad (SM).

[0037] Esta segunda variante ilustrada en la figura 2 permite obtener una seguridad acrecentada del proceso a través de un código de compra (CA_{P1}) más evolucionado que no depende únicamente del producto comprado (P1) sino también del módulo de seguridad (SM). En efecto, este último calcula este código (CA_{P1}) a partir de los identificadores del producto (ID_{P1}) y del del módulo de seguridad (ID_{SM}) al encriptarlos con una clave personal (Kp) de la unidad de usuario (STB). El criptograma Kp(ID_{P1}, ID_{SM}) o código de compra (CA_{P1}) obtenido se muestra en los medios de visualización disponibles con el fin de transmitirse al centro de gestión (CG) por el canal de comunicación. Cabe señalar que la clave personal (Kp) puede ser tanto de tipo simétrico, como asimétrico.

[0038] El centro (CG) encauza la solicitud RQ(ID_{SM}, CA_{P1}, ID_{P1}) hacia el sistema de control de acceso (CAS) para la verificación de la conformidad de los identificadores de usuario del módulo de seguridad (ID_{SM}) y del producto (ID_{P1}) así como del código de compra (CA_{P1}). Este último es recalculado por el sistema de control de acceso (CAS) después de compararse con el que contiene la solicitud.

[0039] Cuando la validez del contenido del criptograma Kp(ID_{P1}, ID_{SM}) se establece, el sistema de control de acceso (CAS) genera un mensaje de confirmación condicional (CEMM) que contiene el derecho definitivo (D1) y un identificador de usuario del derecho temporal (D1t) como condición de aceptación del mensaje.

[0040] Este mensaje (CEMM) es preferiblemente encriptado por una clave personal en dicho módulo de seguridad (SM). Como en la primera variante, el derecho (D1) del mensaje de confirmación (CEMM) reemplaza el derecho temporal (D1t) cuando el identificador de usuario temporal es correcto. Este derecho (D1) definitivo permite el acceso al producto (P1) comprado.

[0041] En caso de que el mensaje (CEMM) no sea recibido por la unidad de usuario (STB) o no sea transmitido por el centro de gestión, el derecho temporal (D1t) expira ya sea al cabo de un período predeterminado de no recepción del mensaje después la creación de este derecho (D1t), o en el momento de la difusión del producto (P1) que crea este derecho (D1t). En esta variante, el código del producto registrado en el momento de la compra contiene información sobre la fecha y la hora de difusión. Cuando el derecho temporal (D1t) vence, el soporte del crédito restante del módulo de seguridad se restablece al valor inicial de antes de la compra del producto (P1) permitiendo de este modo que se ejecute en el módulo de seguridad una nueva validación de acceso a un producto.

[0042] Cuando la verificación no se logra, el sistema de control de acceso (CAS) no genera ningún mensaje (CEMM). Si el criptograma $Kp(ID_{P1}, ID_{SM})$ es incorrecto, no se envía ningún mensaje (CEMM) y el derecho temporal (D1t) persiste hasta su vencimiento. En ambos casos, el acceso al producto (P1) "precomprado" permanece estando prohibido por la ausencia de un derecho (D1) definitivo en el módulo de seguridad (SM).

[0043] Las dos variantes permiten al sistema de control de acceso (CAS) almacenar respectivamente los identificadores de usuario (ID_{SM}, ID_{P1}) del módulo de seguridad (SM) y del producto comprado (P1) en una base de datos (DB). Este registro tendrá lugar preferentemente cuando la verificación del código de producto (CP1) respectivamente del código de compra (CA_{P1}) se haya logrado. Permite establecer un historial, cuentas y estadísticas de los productos comprados por las unidades de usuarios con el fin de retribuir a los proveedores de los productos.

[0044] Un método simplificado consiste en transmitir al centro de gestión información representativa del crédito. Antes de una compra, el usuario solicita que se genere un código de compra en la unidad de usuario. Este código está formado por el crédito restante y el identificador de usuario del módulo de seguridad. También puede estar completado por un valor temporal tal como la fecha.

[0045] Este código es transmitido por el usuario con el identificador de usuario de su módulo de seguridad y el del producto que desea adquirir. El sistema de control de acceso o el centro de gestión extrae del código el valor del crédito en función del identificador de usuario del módulo de seguridad recibido. Si el crédito es suficiente con respecto al valor del producto, un mensaje de compra correspondiente, que contiene el derecho y el importe del producto, se envía al módulo de seguridad. Este verifica que efectivamente el crédito es suficiente para el producto deseado antes de memorizar el derecho y de este modo permitir el acceso al producto.

[0046] Cabe señalar que este método simplificado no es más seguro que la primera variante de la figura 1 ya que es igualmente vulnerable al ataque consistente en saturar el sistema de control de acceso como se ha descrito anteriormente.

REIVINDICACIONES

1. Método de validación de acceso a un producto (P1), por un módulo de seguridad (SM) asociado a una unidad de usuario (STB) conectada, de manera unidireccional, a un sistema de control de acceso (CAS) que transmite mensajes de gestión destinados a dicho módulo de seguridad (SM), donde dichos mensajes son generados por el sistema de control de acceso (CAS) después de la recepción de una solicitud de un derecho de acceso a un producto que consiste en datos digitales difundidos, dicho método que comprende las etapas siguientes:

- compra de un producto (P1) propuesto por la unidad de usuario y verificación por el módulo de seguridad (SM), de que el importe asociado al producto (P1) está cubierto por un crédito restante,
- inscripción de un derecho temporal (D1t) en el módulo de seguridad (SM) cuando el crédito restante es igual o superior al importe asociado a dicho producto (P1),
- determinación de un código (CP1) representativo del producto (P1) comprado,
- formación de una solicitud (RQ) que comprende al menos dicho código (CP1) y un identificador de usuario (ID_{SM}) del módulo de seguridad (SM),
- transmisión a un centro de gestión (CG) asociado al sistema de control de acceso (CAS), a través de un canal independiente a la unidad de usuario (STB), de la solicitud (RQ)
- verificación por el sistema de control de acceso (CAS) de la validez del código (CP1) y del identificador de usuario del módulo de seguridad (ID_{SM}), generación y transmisión de un mensaje de confirmación de derecho (CEMM) que comprende un código de producto (CP1') a la unidad de usuario (STB) asociada a dicho módulo de seguridad (SM) únicamente si la verificación de la validez del código (CP1) y del identificador del módulo de seguridad (IDSM) se logra,

método **caracterizado por el hecho de que** dicho derecho temporal (D1t) es reemplazado por un derecho definitivo (D1) cuando el mensaje de confirmación de derecho (CEMM) transmitido por el sistema de control de acceso (CAS) es recibido por la unidad de usuario (STB) y cuando el código de producto (CP1') corresponde al producto (P1) comprado, donde dicho derecho definitivo (D1) autoriza el acceso al producto (P1) comprado debitando el importe asociado a dicho producto (P1).

2. Método según la reivindicación 1, **caracterizado por el hecho de que** el código de producto (CP1') corresponde al código (CP1) que se transmite en la solicitud dirigida al centro de gestión.

3. Método según una de las reivindicaciones 1 o 2, **caracterizado por el hecho de que** el código (CP1) está contenido en un mensaje de gestión general relativo al producto (P1) distribuido o por distribuir.

4. Método según una de las reivindicaciones 1 a 3, **caracterizado por el hecho de que** la solicitud (RQ) se transmite al centro de gestión (CG) bien por teléfono como mensaje corto o por medio de un servidor vocal, o bien por correo electrónico o cualquier otro canal soportado por el centro de gestión.

5. Método según una de las reivindicaciones 1 o 2, **caracterizado por el hecho de que** el código consiste en un criptograma Kp(ID_{SM}, IDP1), formado por un identificador de usuario (IDP1) del producto (P1) comprado y el identificador de usuario (ID_{SM}) del módulo de seguridad (SM) encriptados con una clave (Kp) personal de la unidad de usuario (STB).

6. Método según la reivindicación 4 **caracterizado por el hecho de que** la solicitud (RQ) comprende asimismo el identificador (IDP1) del producto (P1) comprado.

7. Método según las reivindicaciones 1 a 6, **caracterizado por el hecho de que** el sistema de control de acceso (CAS) verifica la conformidad del código (CP1) o del criptograma Kp(ID_{SM}, IDP1) y la conformidad del identificador de usuario del módulo de seguridad (SM) y autoriza el envío del mensaje de conformación (CEMM) a dicho módulo de seguridad (SM) únicamente si la verificación es positiva.

8. Método según las reivindicaciones 5 a 7, **caracterizado por el hecho de que** el sistema de control de acceso (CAS), al recibir la solicitud (RQ), recalcula el criptograma Kp(ID_{SM}, IDP1) a partir de los identificadores (ID_{SM};, IDP1) del módulo de seguridad y del producto y lo compara con el criptograma contenido en la solicitud (RQ), cuando el resultado de la comparación es positiva, el sistema de control de acceso (CAS) transmite un mensaje de confirmación (CEMM) que contiene un derecho definitivo (D1) y un identificador de usuario del derecho temporal (D1t) como condición de aprobación de dicho mensaje.

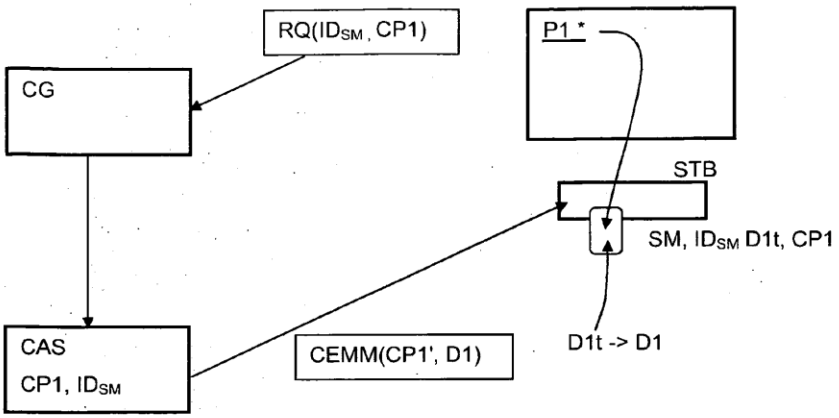
RQ(ID$_{SM}$, CP1)
CG
P1 *
STB
SM, ID$_{SM}$ D1t, CP1
CAS
CP1, ID$_{SM}$
CEMM(CP1', D1)
D1t -> D1

Fig. 1

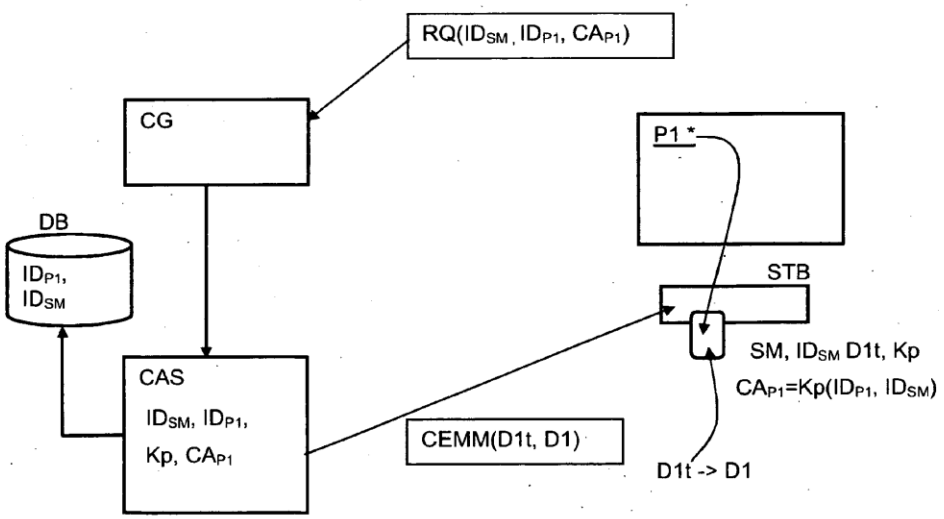
RQ(ID$_{SM}$, ID$_{P1}$, CA$_{P1}$)
CG
P1 *
DB
ID$_{P1}$,
ID$_{SM}$
STB
SM, ID$_{SM}$ D1t, Kp
CA$_{P1}$=Kp(ID$_{P1}$, ID$_{SM}$)
CAS
ID$_{SM}$, ID$_{P1}$,
Kp, CA$_{P1}$
CEMM(D1t, D1)
D1t -> D1

Fig. 2