(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 744 269**

(51) Int. CI.:

G06Q 20/20 (2012.01)
G06Q 20/32 (2012.01)
G06Q 20/38 (2012.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **14.04.2015 E 15163461 (5)**

(97) Fecha y número de publicación de la concesión europea: **05.06.2019 EP 2933767**

(54) Título: **Procedimiento de desactivación de un módulo de pago, producto de programa de ordenador, medio de almacenamiento y módulo de pago correspondientes**

(30) Prioridad:

18.04.2014 FR 1453543

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
24.02.2020

(73) Titular/es:

INGENICO GROUP (100.0%)
28-32 Boulevard de Grenelle
75015 Paris, FR

(72) Inventor/es:

NACCACHE, DAVID;
QUENTIN, PIERRE;
GHILIOTTO-YOUNG, DORINA y
BRIER, ERIC M.

(74) Agente/Representante:

ELZABURU, S.L.P

DESCRIPCIÓN

Procedimiento de desactivación de un módulo de pago, producto de programa de ordenador, medio de almacenamiento y módulo de pago correspondientes

1 Campo de la invención

La presente invención se refiere al campo de la desactivación definitiva de un módulo de pago y, más en particular, de un módulo de pago vinculable (por ejemplo, conectado o integrado) a un terminal de comunicación.

2 Soluciones de la técnica anterior

La desactivación de un módulo de pago vinculable a un terminal de comunicación debe permitir garantizar una seguridad máxima de utilización de este módulo de pago, impidiendo toda ulterior utilización de tal módulo de pago desactivado e impidiendo todo acceso a datos sensibles anteriormente utilizados o almacenados por tal módulo de pago desactivado.

Por ejemplo, cuando se integra un módulo de pago en un terminal de comunicación de un usuario, el mismo puede solicitar la desactivación definitiva del módulo de pago, antes de desprenderse (prestar o vender) de su terminal de comunicación, al objeto de que un tercero no pueda tener acceso a datos sensibles (por ejemplo, el número de su tarjeta bancaria) utilizados o almacenados con anterioridad por el módulo de pago.

Consiste una solución convencional (véase, por ejemplo, el documento US 2011/0270741) en borrar toda la memoria del módulo de pago cuando se pretende desactivar este último, al objeto de impedir su ulterior funcionamiento y de impedir el acceso a datos almacenados en esta memoria. Puede utilizarse a continuación un programa de soporte lógico para verificar que efectivamente se ha borrado la memoria.

En cambio, un gran inconveniente de esta solución radica en la imposibilidad de asegurarse de que un programa fraudulento no haya “tomado el control” para simular este borrado de la memoria, así como la ulterior verificación.

Existe, por tanto, una necesidad de una solución que permita asegurarse de que el módulo de pago está desactivado definitivamente y de que ningún dato sensible es accesible a partir del instante en que queda desactivado el módulo de pago.

3 Sumario de la invención

La invención concierne a un procedimiento de desactivación de un módulo de pago vinculable a un terminal de comunicación, que comprende las dos siguientes fases:

- una fase de desactivación que comprende al menos una etapa de borrado de toda la memoria del módulo de pago, a excepción de un área de memoria no volátil en la que se almacena una clave de encriptación *k*, llamándose a dicha memoria borrada memoria principal y no estando disponible dicha clave de encriptación *k* sino cuando la memoria principal del módulo de pago está vacía;
- al menos una fase de verificación de la desactivación que comprende las siguientes etapas:
    - una etapa de verificación de que la memoria principal está vacía, que suministra un resultado de verificación positivo o negativo;
    - si el resultado de verificación es positivo:
        - una etapa de cálculo de una respuesta a un desafío recibido con anterioridad por el módulo de pago con origen en una entidad diferenciada del módulo de pago, llevándose a la práctica el cálculo con el concurso de la clave de encriptación *k*;
        - una etapa de transmisión de la respuesta a la entidad.

De este modo, de acuerdo con sus diferentes formas de realización, la invención propone una solución novedosa e inventiva de desactivación de un módulo de pago vinculable a un terminal de comunicación, que permite asegurarse de manera segura de que el módulo se ha desactivado efectivamente, por lo que ya no es utilizable, y de que todos los datos sensibles que anteriormente había podido utilizar o almacenar se han borrado realmente de la memoria del módulo desactivado.

Para conseguir esto, el proceso de desactivación incluye dos fases sucesivas: una fase de desactivación propiamente dicha del módulo de pago, que consiste en borrar la memoria principal del módulo de pago, y una fase de verificación de la desactivación. Esta segunda fase de verificación de la desactivación es segura y garantiza la desactivación del módulo de pago, ya que pone en práctica un parámetro particular, denotado como clave de encriptación *k*, almacenado en una parte específica no volátil de la memoria del módulo de pago y que no es accesible, a través de un comando de utilización, sino cuando se ha borrado todo el resto de la memoria (denotada

como memoria principal) del módulo de pago.

De este modo, si no es borrada por completo la memoria principal, la fase de verificación es fallida, ya que el comando de utilización de la clave de encriptación *k* necesaria para esta verificación no está disponible.

En efecto, la fase de verificación comprende, primero, una etapa de verificación de que la memoria principal está vacía, por ejemplo utilizando un programa conocido de verificación del contenido de una memoria, que suministra un resultado de verificación, positivo o negativo.

Si este resultado es positivo, la fase de verificación comprende a continuación una etapa de cálculo de una respuesta a un desafío transmitido al módulo de pago por una entidad diferenciada. Este cálculo de una respuesta al desafío recibido utiliza la clave de encriptación *k*, vuelta accesible mediante el borrado de la memoria principal del módulo de pago. Esta respuesta al desafío es transmitida entonces, por el módulo de pago, a la entidad diferenciada que ha transmitido el desafío. Esta entidad, entonces, puede validar que la desactivación del módulo de pago es efectiva, verificando que la respuesta al desafío es correcta.

Si el resultado de verificación es negativo, la clave de encriptación *k* no es accesible y, entonces, conviene tratar nuevamente de borrar la memoria principal del módulo de pago.

Es de señalar que la fase de verificación puede ser reiterada, por ejemplo cuando se pretende verificar, algún tiempo después de la desactivación definitiva de un módulo de pago, que el mismo no ha sido reactivado de manera fraudulenta.

De acuerdo con una característica de la invención, la fase de desactivación se dispara mediante la recepción, por parte del módulo de pago, de al menos una petición de desactivación recibida con origen en la entidad.

La mayoría de las veces, la desactivación de tal módulo de pago es solicitada por el usuario de ese módulo de pago, por mediación de su terminal de comunicación, por ejemplo cuando está pensando en prestar o vender su terminal de comunicación. En este caso, el usuario solicita la desactivación del módulo de pago a través de la aplicación dedicada a la administración de este módulo de pago. La entidad diferenciada que solicita la desactivación del módulo de pago se corresponde entonces con esta aplicación de administración del módulo de pago, y el resultado de esta fase de verificación de la desactivación del módulo de pago se puede transmitir entonces al servidor seguro intermediario (servidor pasarela) a cargo del establecimiento de un vínculo seguro entre el módulo de pago y el servidor de comercio, dentro del ámbito de un pago remoto.

Puede asimismo ocurrir que se necesite la desactivación del módulo de pago cuando es detectado un uso fraudulento de este módulo de pago, por ejemplo directamente por el servidor intermediario seguro, que constituye, en este caso, la entidad diferenciada solicitante de la desactivación del módulo de pago.

En particular, la clave de encriptación *k* almacenada en la memoria no volátil del módulo de pago nunca es accesible a efectos de lectura.

De este modo, la clave de encriptación *k* nunca puede ser utilizada fraudulentamente para transmitir una respuesta a un desafío cuando la memoria principal del módulo de pago no está totalmente vacía. En efecto, al no ser nunca accesible a efectos de lectura, no puede ser “recuperada” en ningún momento, en vistas a una ulterior utilización para simular un funcionamiento normal de respuesta a un desafío.

Esto constituye una doble seguridad con la característica consistente en no hacer utilizable esta clave de encriptación *k* sino cuando la memoria principal del módulo de pago realmente está vacía.

De este modo, no sólo el comando de utilización de la clave de encriptación *k* no está disponible sino cuando la memoria principal del módulo de pago está vacía, sino que la propia clave de encriptación nunca es accesible a efectos de lectura (tan sólo puede ser utilizada a través de su comando para el cálculo de una respuesta a un desafío).

De acuerdo con un aspecto particular de la invención, el cálculo de una respuesta a un desafío utiliza asimismo al menos un dato representativo de la petición de desactivación, perteneciendo la información al grupo que comprende:

- un identificador de la entidad;
- un sellado de tiempo de la petición de desactivación.

De este modo, el cálculo de la respuesta al desafío también tiene en cuenta datos referentes a la petición de desactivación. Por ejemplo, los datos cifrados mediante la clave de encriptación *k* se constituyen no sólo a partir del desafío, sino también de un identificador de la entidad que ha solicitado la desactivación, así como de la fecha y la hora de esta petición de desactivación. Esto permite una verificación suplementaria, en la entidad (por ejemplo, el servidor pasarela) receptora de la respuesta al desafío, de la autenticidad de esta respuesta.

De acuerdo con una forma particular de realización de la invención, la fase de desactivación se dispara después de

una etapa de validación de la autorización de la entidad para desactivar el módulo de pago.

Por lo tanto, se pone en práctica asimismo un control previo para asegurarse de que la entidad solicitante de la desactivación del módulo de pago está autorizada efectivamente a hacerlo. Si esta verificación es positiva, entonces se ponen en práctica las fases de desactivación y de verificación.

Asimismo, la invención concierne a un módulo de pago vinculable a un terminal de comunicación, que comprende unos medios de desactivación que comprenden:

- medios de borrado de toda la memoria del módulo de pago, llamada memoria principal, a excepción de un área de memoria no volátil en la que se almacena una clave de encriptación *k*, no estando disponible la clave de encriptación *k* sino cuando la memoria principal del módulo de pago está vacía;
- medios de verificación de que la memoria principal está vacía, que suministran un resultado de verificación positivo o negativo;
- medios de cálculo de una respuesta a un desafío recibido con anterioridad por el módulo de pago con origen en una entidad diferenciada del módulo de pago, llevándose a la práctica el cálculo con el concurso de la clave de encriptación *k*, siendo activados los medios de cálculo por un resultado de verificación positivo;
- medios de transmisión de la respuesta a la entidad.

Asimismo, la invención concierne a un programa de ordenador descargable desde una red de comunicación y/o almacenado en un soporte legible por ordenador y/o ejecutable por un procesador, que comprende instrucciones de código de programa para la ejecución del procedimiento tal y como se ha descrito anteriormente, cuando es ejecutado por un procesador. Este programa puede utilizar cualquier lenguaje de programación y materializarse en forma de código fuente, código objeto, o de código intermedio entre código fuente y código objeto, tal como en una forma compilada parcialmente, o en cualquier otra forma deseable.

Finalmente, la invención concierne a un medio de almacenamiento, o soporte de información, legible por ordenador y no transitorio, que almacena un programa de ordenador que comprende un juego de instrucciones ejecutables por un ordenador o un procesador para poner en práctica el procedimiento tal y como se ha descrito anteriormente. El soporte de información puede corresponder a cualquier entidad o dispositivo capaz de almacenar el programa. Por ejemplo, el soporte puede incluir un medio de almacenamiento, tal como una ROM, por ejemplo un CD-ROM o una ROM de circuito microelectrónico, o también un medio de registro magnético, por ejemplo un disquete (floppy disc) o un disco duro. Por otra parte, el soporte de información puede corresponder a un soporte transmisible, tal como una señal eléctrica u óptica, que se puede conducir a través de un cable eléctrico u óptico, por radio o por otros medios. El programa según la invención se puede descargar en particular por una red de tipo Internet. Alternativamente, el soporte de información puede corresponder a un circuito integrado en el que va incorporado el programa, estando adaptado el circuito para ejecutar o para ser utilizado en la ejecución del procedimiento en cuestión.

4 Lista de figuras

Otras características y ventajas de la invención se pondrán más claramente de manifiesto con la lectura de la siguiente descripción de una forma particular de realización, dada a título de mero ejemplo ilustrativo y no limitativo, y de los dibujos que se acompañan, de los cuales:

- la figura 1 presenta las principales etapas de un procedimiento de desactivación de un módulo de pago según una primera forma de realización de la invención; y

- las figuras 2a y 2b ilustran un ejemplo de módulo de pago según una forma de realización de la invención.

5 Descripción detallada de la invención

5.1 Principio general

Consiste el principio de la invención en proporcionar una técnica de desactivación verificable de un módulo de pago vinculable a un terminal de comunicación, que permita asegurarse de que el módulo es desactivado definitivamente, en el sentido de que ya no es utilizable para una operación de pago y en el que ya no son accesibles los eventuales datos sensibles utilizados o almacenados con anterioridad.

Por otro lado, la técnica de desactivación de un módulo de pago según las diferentes formas de realización de la invención permite verificar, en todo momento, que un módulo de pago está desactivado efectivamente.

Esta técnica la lleva a la práctica el propio módulo de pago y, en cierto modo, constituye una autodesactivación verificable segura.

Las diferentes formas de realización de la invención que pasamos a describir son de más particular aplicación en un módulo de pago que comprende mecanismos de seguridad propios de un terminal de pago convencional y capaz de

procesar una transacción mediante tarjeta de microcircuito o mediante tarjeta virtual. Este módulo de pago está, por ejemplo, conectado a o integrado en el terminal de comunicación (PC, tableta, teléfono inteligente...) de un usuario.

Es obvio que la invención no se limita a este tipo de módulos de pago, sino que asimismo es de aplicación en todo dispositivo que deba responder a la misma problemática de desactivación segura y verificable.

5.2 Descripción de una forma de realización

La figura 1 ilustra las principales etapas de un procedimiento de desactivación según una forma de realización de la invención, en el que se debe desactivar de manera segura y verificable un módulo de pago.

El procedimiento de desactivación comprende dos fases sucesivas: una fase de desactivación 10 y una fase de verificación 11 de la desactivación.

En la mayoría de los casos, estas dos fases se suceden, en orden a asegurarse de que se ha desactivado efectivamente un módulo de pago. Puede asimismo ocurrir que se reitere la fase de verificación de la desactivación, cuando se pretende asegurarse nuevamente de que efectivamente el módulo de pago ha sido desactivado con anterioridad.

Por lo tanto, la primera fase de desactivación 10 consiste principalmente en borrar, en una etapa 100, todos los datos almacenados en la memoria principal del módulo de pago, es decir, todos los datos sensibles necesarios para una operación de pago (tales como el número de tarjeta bancaria del usuario, así como, eventualmente, datos relativos a cada una de las operaciones de pago efectuadas mediante el módulo de pago,...).

De acuerdo con una forma de realización de la invención, esta fase de desactivación 10 se dispara mediante una petición de desactivación, emitida por una entidad diferenciada del módulo de pago.

Por ejemplo, esta entidad se halla asimismo integrada en el terminal de comunicación del usuario y corresponde a un módulo de administración/gestión del módulo de pago, accesible por el usuario y que especialmente brinda una funcionalidad de desactivación del módulo de pago. De este modo, el usuario del terminal de comunicación que lleva integrado el módulo de pago puede decidir desactivar este último cuando está pensando en confiar su terminal de comunicación a un tercero. Este módulo de administración puede estar, en este caso, unido a un servidor intermediario seguro (servidor pasarela) a cargo del establecimiento de un vínculo seguro entre el módulo de pago y el servidor de comercio, dentro del ámbito de un pago remoto.

De acuerdo con otro ejemplo, la entidad corresponde a este propio servidor pasarela, apto para transmitir una petición de desactivación al módulo de pago.

De acuerdo con una forma particular de realización de la invención, la fase de desactivación 10 no se pone en práctica, tras la recepción de la petición de desactivación por el módulo de pago, sino cuando este último ha verificado con anterioridad que la entidad origen de la petición está autorizada a solicitar tal desactivación.

Por ejemplo, el módulo de pago puede estar en conocimiento de una o varias entidades autorizadas a solicitar su desactivación (en forma de una lista de identificadores en memoria, por ejemplo) y la petición de desactivación puede contener un identificador de la entidad emisora, permitiendo así al módulo de pago comparar este identificador con los de su lista. Cuando el módulo de pago no reconoce la entidad emisora de la petición en calidad de entidad autorizada, no se ponen en práctica las fases de desactivación y de verificación.

De acuerdo con las diferentes formas de realización de la invención, la memoria principal del módulo de pago se distingue de un área de memoria no volátil también presente en el módulo de pago y utilizada únicamente para almacenar un dato específico, denominado clave de encriptación *k*, que sirve para la segunda fase de verificación de la desactivación.

De acuerdo con las diferentes formas de realización de la invención, esta clave de encriptación *k* nunca es accesible a efectos de lectura y su comando de utilización no está disponible sino cuando la memoria principal del módulo de pago está completamente vacía. De este modo, esta clave *k* no puede ser utilizada fraudulentamente por un programa de soporte lógico o un módulo de soporte físico para simular una verificación de desactivación mientras que la memoria principal del módulo no está vacía.

Cuando se termina la fase de desactivación 10, se pone en práctica una fase de verificación 11 de esta desactivación, empezando por una etapa de verificación 110 del borrado de la memoria principal.

Esta etapa de verificación 110 puede poner en práctica, por ejemplo, una técnica conocida de verificación por equipo lógico del borrado de una memoria y suministrar un resultado de verificación, positivo si la memoria principal del módulo de pago sí que está vacía, o negativo cuando la memoria no está vacía (cuando el borrado ha sido fallido o también cuando la etapa de borrado se ha manipulado fraudulentamente al objeto de no borrar nada).

Cuando el resultado de verificación es negativo, el módulo de pago informa de ello a la entidad origen de la iniciativa de desactivación. Por ejemplo, el módulo de pago transmite un mensaje de resultado de verificación negativo o, por

el contrario, la ausencia de mensaje previsto en el caso de un resultado de verificación positivo permite que la entidad sea informada de un resultado de verificación negativo.

De este modo, de acuerdo con una forma de realización de la invención, cuando el resultado de verificación es positivo, la entidad origen de la iniciativa de desactivación recibe un mensaje de resultado de verificación positivo y, entonces, emite un desafío con destino al módulo de pago, para la puesta en práctica de la siguiente etapa 111 de la fase de verificación 11.

De acuerdo con otra forma de realización, es transmitido un desafío por la entidad origen de la iniciativa de desactivación en el instante de la petición de desactivación, por ejemplo, y cuando el resultado de verificación es positivo, el módulo de pago pone en práctica directamente la etapa de cálculo 111 de una respuesta al desafío recibido con anterioridad.

Por lo tanto, esta etapa 111 no es puesta en práctica por el módulo de pago sino cuando se ha asegurado previamente de que su memoria principal estaba vacía. Además, esta etapa 111 no se puede poner en práctica concretamente sino cuando esta memoria principal está vacía, ya que la clave de encriptación *k* no es accesible, para el cálculo de una respuesta a un desafío, sino cuando la memoria principal del módulo de pago está vacía.

De este modo, si no se cumple esta condición, el comando de utilización de la clave de encriptación *k* no está disponible, y el módulo de pago no puede calcular una respuesta al desafío. En este caso, en ausencia de respuesta, por parte del módulo de pago, al desafío transmitido con anterioridad, la entidad origen de la iniciativa de desactivación comprende que la desactivación del módulo de pago no se ha desarrollado correctamente.

Por el contrario, cuando efectivamente se ha borrado por completo la memoria principal del módulo de pago, se puede poner en práctica la etapa de cálculo 111 de una respuesta al desafío. Por ejemplo, este cálculo consiste en una encriptación del desafío mediante la clave de encriptación *k*, vuelta accesible a causa del borrado previo de la memoria principal. De este modo, el comando de utilización de esta clave de encriptación *k* para encriptar el desafío se encuentra disponible, por lo que se puede calcular una respuesta al desafío.

De acuerdo con una variante de realización, se pueden encriptar asimismo otros datos, además del desafío, mediante la clave de encriptación *k*. Por ejemplo, se pueden encriptar, con el desafío, datos representativos de la entidad origen de la iniciativa de petición de desactivación (por ejemplo, un identificador de esta entidad) y/o del sellado de tiempo de esta petición. El módulo de pago tiene conocimiento de estos datos por intermedio de su transmisión por la propia entidad, o por intermedio de otros medios (sellado de tiempo disponible por intermedio del terminal de comunicación al que está vinculado el módulo de pago, por ejemplo).

Esta respuesta al desafío, una vez calculada, se transmite, en una etapa de transmisión 112, a la entidad origen de la iniciativa de petición de desactivación. Así, esta entidad puede verificar que la desactivación del módulo de pago se ha desarrollado debidamente, si la respuesta al desafío se corresponde con la esperada. En efecto, si esta respuesta es correcta, la entidad origen de la iniciativa de petición de desactivación puede tener la seguridad de que el módulo de pago ha sido desactivado de manera segura y de que ningún dato sensible ya no es accesible por intermedio de su memoria. Si la respuesta al desafío no es correcta, se puede disparar nuevamente una desactivación o puede emitirse una alerta.

5.3 Descripción de un ejemplo de módulo de pago

La figura 2a ilustra un ejemplo de módulo de pago 20 según una forma de realización de la invención, que especialmente presenta unos medios de desactivación y de verificación de esta desactivación.

Por ejemplo, tal módulo de pago 20, que puede estar conectado a o integrado en el terminal de comunicación (PC, tableta, teléfono inteligente...) de un usuario, comprende mecanismos de seguridad propios de un terminal de pago convencional y es capaz de procesar una transacción mediante tarjeta de microcircuito o mediante tarjeta virtual. Por lo tanto, se puede hacer, en especial, que almacene datos sensibles, como un número de tarjeta bancaria o datos relativos a una transacción en particular. Por motivos de seguridad ligados al ámbito bancario, tal módulo de pago debe poderse desactivar con seguridad y de manera verificable, de modo que, una vez desactivado, ya no pueda ser utilizado y que los datos que había podido memorizar ya no sean accesibles.

De este modo, de acuerdo con las diferentes formas de realización de la invención, tal módulo de pago 20 comprende medios de borrado 200 de su memoria principal, es decir, toda la memoria utilizada para almacenar datos sensibles (por ejemplo, números de tarjeta bancaria, de cuenta bancaria, certificados...), así como medios de verificación 201 de este borrado. Estos medios de borrado 200 y de verificación del borrado 201 se pueden llevar a la práctica mediante la ejecución de uno o varios programas de soporte lógico conocidos.

Por otro lado, el módulo de pago 20 presenta asimismo unos medios (no representados) de recepción de una petición de desactivación, emitida por una entidad diferenciada (no representada) del módulo de pago 20, que especialmente activan los medios de borrado 200.

De acuerdo con las formas de realización de la invención, el módulo de pago 20 presenta asimismo unos medios de

cálculo 202 de una respuesta a un desafío recibido con anterioridad (por ejemplo, a través de unos medios, no representados, de recepción de tal desafío). Estos medios de cálculo 202 de una respuesta a un desafío ponen en práctica uno o varios algoritmos (conocidos) de encriptación del desafío, especialmente con el concurso de una clave de encriptación *k* almacenada en un área no volátil de la memoria (no representada) del módulo de pago 20. Estos medios de cálculo 202 se activan a la recepción de un resultado de verificación positivo, emitido por los medios de verificación 201 por ejemplo, que confirma que la memoria principal del módulo de pago 20 efectivamente ha sido borrada por completo por los medios de borrado 200. Además, el comando de utilización de la clave de encriptación *k* no está disponible sino cuando esta memoria principal está efectivamente vacía.

De este modo, los medios de cálculo 202 no pueden calcular una respuesta a un desafío sino cuando la memoria principal del módulo de pago 20 está vacía, permitiendo así asegurarse de que efectivamente el módulo ha sido desactivado.

La respuesta al desafío se transmite a continuación, por intermedio de unos medios de transmisión 203, a la entidad origen de la iniciativa de petición de desactivación.

Esta respuesta, una vez transmitida por el módulo de pago 20, esta entidad diferenciada del módulo de pago 20 puede verificar que efectivamente corresponde al desafío transmitido con anterioridad al módulo de pago. Si es así, la entidad origen de la iniciativa de petición de desactivación puede tener la seguridad de que el módulo de pago ha sido desactivado de manera segura y de que ningún dato sensible ya no es accesible por intermedio de su memoria.

Claro es que todas las características antes descritas en relación con las diferentes formas de realización del procedimiento de desactivación son aplicables en el propio módulo de pago.

Además, la figura 2b ilustra de otra manera el módulo de pago 20 que, comprendiendo una memoria 21 constituida a partir de una memoria intermedia, una unidad de proceso 22 equipada, por ejemplo, con un microprocesador, y pilotada por el programa de ordenador 23, pone en práctica un procedimiento de desactivación según las diferentes formas de realización de la invención.

Con la inicialización, es decir, con el encendido del terminal de comunicación al que está vinculado el módulo de pago, las instrucciones de código del programa de ordenador 23 se cargan, por ejemplo, en una memoria, antes de ser ejecutadas por el procesador de la unidad de proceso 22. La unidad de proceso 22 recibe como entrada al menos un dato representativo de una petición de desactivación, y eventualmente un desafío. El microprocesador de la unidad de proceso 22 pone en práctica las etapas del procedimiento de desactivación, según las instrucciones del programa de ordenador 23, para efectuar una desactivación y una verificación de la desactivación del módulo de pago 20.

Comprende para ello el módulo de pago 20, aparte de la memoria intermedia 21, unos medios de comunicación, tales como módulos de comunicaciones en red, medios de transmisión de datos y, eventualmente, un procesador de cifrado apto para poner en práctica algoritmos de criptografía tales como el algoritmo RSA.

En una forma particular de realización de la invención, el módulo de pago 20 del usuario, que puede estar integrado (es decir, físicamente soldado o ligado) a un teléfono inteligente, una tableta, un ordenador portátil, un PDA, integra unos medios de gestión de transacción (no representados). Estos medios pueden materializarse en forma de un procesador particular implementado en el seno del módulo de pago, siendo dicho procesador un procesador seguro.

REIVINDICACIONES

1. Procedimiento de desactivación de un módulo de pago vinculable a un terminal de comunicación, que comprende las dos siguientes fases:

- una fase de desactivación que comprende al menos una etapa de borrado de toda la memoria de dicho módulo de pago, a excepción de un área de memoria no volátil en la que se almacena una clave de encriptación *k*, llamándose a dicha memoria borrada memoria principal y no estando disponible dicha clave de encriptación *k* sino cuando dicha memoria principal de dicho módulo de pago está vacía;

- al menos una fase de verificación de dicha desactivación que comprende las siguientes etapas:

  - una etapa de verificación de que dicha memoria principal está vacía, que suministra un resultado de verificación positivo o negativo;

  - si dicho resultado de verificación es positivo:

    - una etapa de cálculo de una respuesta a un desafío recibido con anterioridad por dicho módulo de pago con origen en una entidad diferenciada de dicho módulo de pago, llevándose a la práctica dicho cálculo con el concurso de dicha clave de encriptación *k*;

    - una etapa de transmisión de dicha respuesta a dicha entidad.

2. Procedimiento de desactivación de un módulo de pago según la reivindicación 1, caracterizado por que dicha fase de desactivación se dispara mediante la recepción, por parte de dicho módulo de pago, de al menos una petición de desactivación con origen en dicha entidad.

3. Procedimiento de desactivación de un módulo de pago según una cualquiera de las reivindicaciones 1 y 2, caracterizado por que dicha clave de encriptación *k* almacenada en dicha memoria no volátil de dicho módulo de pago nunca es accesible a efectos de lectura.

4. Procedimiento de desactivación de un módulo de pago según la reivindicación 2, caracterizado por que dicho cálculo de una respuesta a un desafío utiliza asimismo al menos un dato representativo de dicha petición de desactivación, perteneciendo dicha información al grupo que comprende:

- un identificador de dicha entidad;

- un sellado de tiempo de dicha petición de desactivación.

5. Procedimiento de desactivación de un módulo de pago según una cualquiera de las reivindicaciones 1 a 4, caracterizado por que dicha fase de desactivación se dispara después de una etapa de validación de la autorización de dicha entidad para desactivar dicho módulo de pago.

6. Módulo de pago vinculable a un terminal de comunicación, que comprende unos medios de desactivación que comprenden:

- medios de borrado de toda la memoria de dicho módulo de pago, a excepción de un área de memoria no volátil en la que se almacena una clave de encriptación *k*, llamándose a dicha memoria borrada memoria principal y no estando disponible dicha clave de encriptación *k* sino cuando dicha memoria principal de dicho módulo de pago está vacía;

- medios de verificación de que dicha memoria principal está vacía, que suministran un resultado de verificación positivo o negativo;

- medios de cálculo de una respuesta a un desafío recibido con anterioridad por dicho módulo de pago con origen en una entidad diferenciada de dicho módulo de pago, llevándose a la práctica dicho cálculo con el concurso de dicha clave de encriptación *k*, siendo activados dichos medios de cálculo por un resultado de verificación positivo;

- medios de transmisión de dicha respuesta a dicha entidad.

7. Programa de ordenador descargable desde una red de comunicación y/o almacenado en un soporte legible por ordenador y/o ejecutable por un procesador, caracterizado por comprender instrucciones de código de programa para la ejecución del procedimiento según una cualquiera de las reivindicaciones 1 a 5, cuando es ejecutado por un procesador.

8. Medio de almacenamiento legible por ordenador y no transitorio, que almacena un programa de ordenador que comprende un juego de instrucciones ejecutables por un ordenador o un procesador para poner en práctica el procedimiento según una cualquiera de las reivindicaciones 1 a 5.

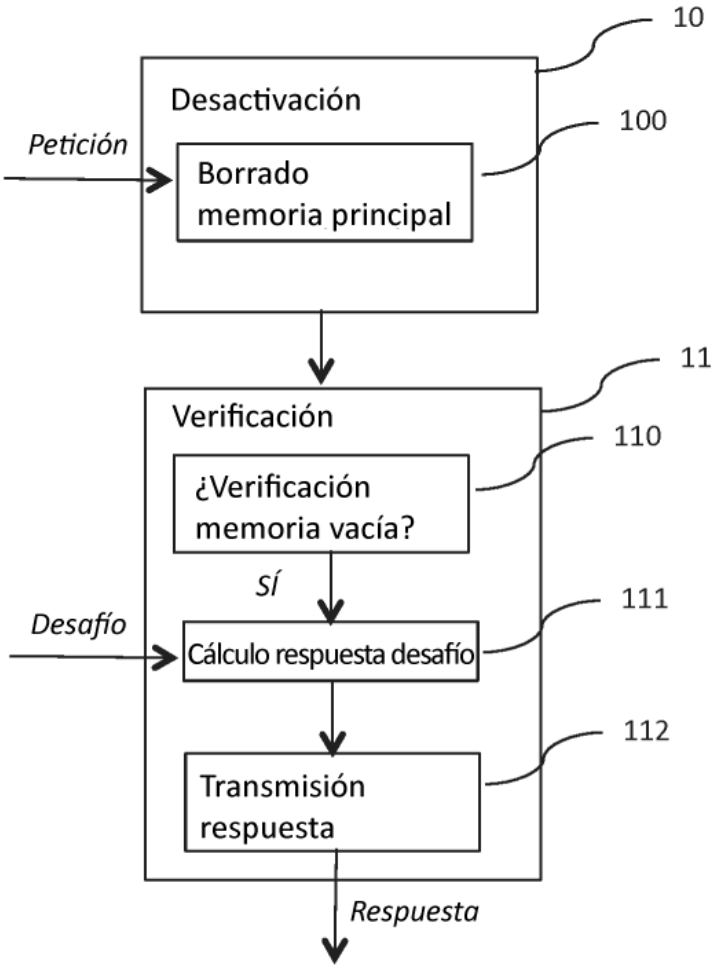
10
Desactivación
Petición
100
Borrado
memoria principal
11
Verificación
110
¿Verificación
memoria vacía?
Sí
Desafío
111
Cálculo respuesta desafío
112
Transmisión
respuesta
Respuesta

Figura 1

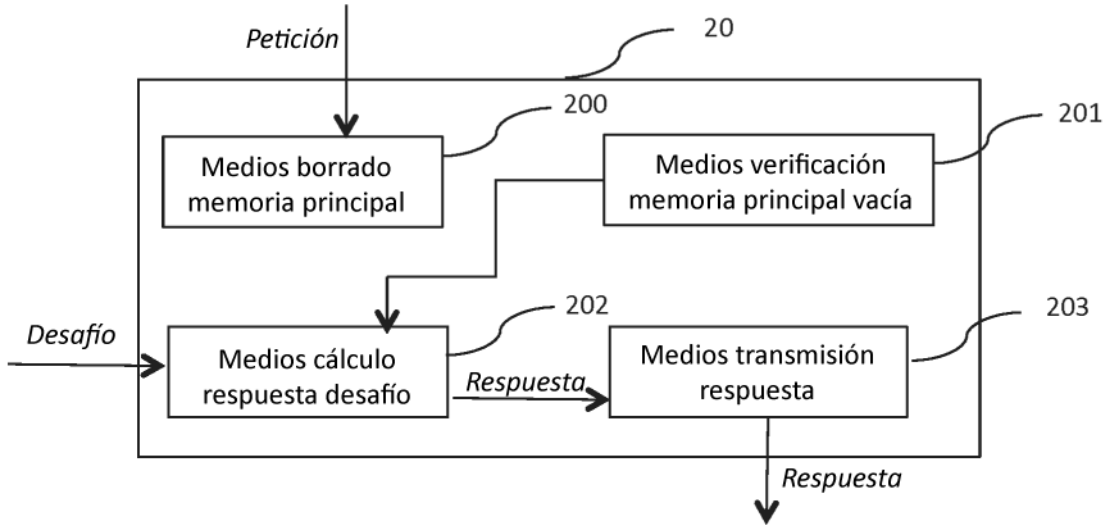

Figura 2a

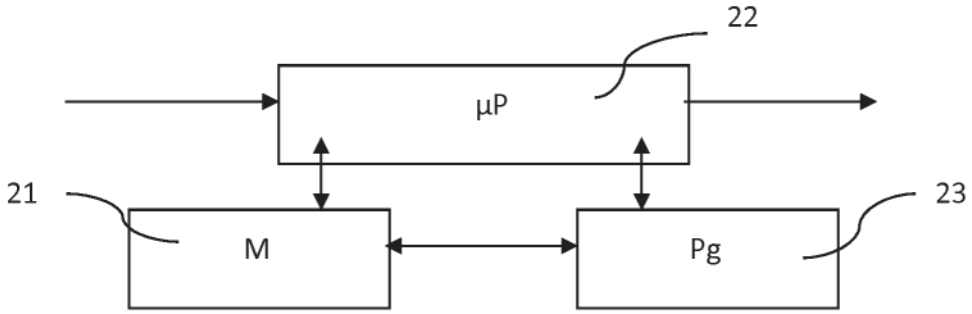

Figura 2b