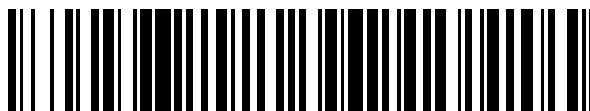


19



OFICINA ESPAÑOLA DE
PATENTES Y MARCAS

ESPAÑA



11 Número de publicación: **2 432 503**

51 Int. Cl.:

G07F 7/10

(2006.01)

12

TRADUCCIÓN DE PATENTE EUROPEA

T3

96 Fecha de presentación y número de la solicitud europea: **06.12.2011** **E 11192137 (5)**

97 Fecha y número de publicación de la concesión europea: **24.07.2013** **EP 2463833**

54 Título: **Procedimiento y dispositivo de control de ejecución para funciones internas y aplicaciones protegidas integradas en tarjetas de microcircuitos para terminales móviles**

30 Prioridad:

09.12.2010 FR 1060288

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

03.12.2013

73 Titular/es:

OBERTHUR TECHNOLOGIES (100.0%)
420 rue d'Estienne d'Orves
92700 Colombes, FR

72 Inventor/es:

RABOISSON, AURÉLIEN y
DENIS, SYLVESTRE

74 Agente/Representante:

PÉREZ BARQUÍN, Eliana

ES 2 432 503 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

Procedimiento y dispositivo de control de ejecución para funciones internas y aplicaciones protegidas integradas en tarjetas de microcircuitos para terminales móviles

5 La presente invención se refiere a la ejecución de funciones en unas tarjetas de microcircuitos y más particularmente a un procedimiento y un dispositivo de control de la ejecución para funciones internas y aplicaciones protegidas integradas en unas tarjetas de microcircuitos para terminales móviles, particularmente unas tarjetas de identificación.

10 El desarrollo de terminales móviles tales como los teléfonos móviles ha implicado el desarrollo de numerosas aplicaciones que no son necesariamente, en sí mismas, unas aplicaciones de telefonía. Entre estas aplicaciones, existen particularmente unas aplicaciones de juegos, de gestión de informaciones personales, de gestión del tiempo, de monedero electrónico, de pago, etc. Una aplicación de pago o de monedero electrónico permite pagar un producto o servicio por medio de su terminal móvil.

15 Según su naturaleza, el acceso a estas aplicaciones o a ciertas de sus funcionalidades puede estar controlado. De ese modo, por ejemplo, las aplicaciones de pago, particularmente para el pago de sumas sustanciales, requieren generalmente una identificación del usuario. Una identificación de ese tipo se puede realizar a partir de una tarjeta de identificación si el terminal móvil utilizado para ejecutar la aplicación dispone de ella.

20 Existen particularmente unas tarjetas de identificación conocidas bajo los nombres de tarjetas SIM (acrónimo de *Subscriber Identity Module* en terminología anglosajona), tarjetas USIM (acrónimo de *Universal Subscriber Identity Module* en terminología anglosajona), tarjetas UICC (acrónimo de *UMTS Integrated Circuit Card* en terminología anglosajona, siendo UMTS la sigla de *Universal Mobile Telecommunications System* en terminología anglosajona) y tarjetas RUIM (acrónimo de *Removable Universal Identity Module* en terminología anglosajona).

30 Estas tarjetas comprenden generalmente unos medios de tratamiento de datos y unos medios de memorización de los datos para el almacenamiento de informaciones específicas para un usuario de una red de telefonía móvil. La presencia de una tarjeta de este tipo en el seno de un terminal móvil, en particular de un teléfono móvil, permite a este terminal, gracias a las informaciones contenidas en la tarjeta de identificación, conectarse a la red e intercambiar unos datos con otros terminales de la red, particularmente de manera segura (la tarjeta contiene por ejemplo una clave criptográfica que permite autenticarse ante la red y codificar unos intercambios de datos).

35 Las tarjetas de identificación forman un elemento seguro de los terminales móviles que permiten una autenticación de los usuarios de estas tarjetas gracias a unas claves de autenticación memorizadas, por ejemplo, en los medios de memorización de esas tarjetas.

40 Por otro lado, ciertos terminales móviles disponen de medios de comunicación inalámbrica de alcance reducido, por ejemplo del tipo NFC (siglas de *Near Field Communication* en terminología no sajona). Los terminales móviles comprenden entonces una antena de comunicación de campo cercano. Esta antena puede estar integrada igualmente en una tarjeta extraíble del terminal. Permite intercambiar datos entre el terminal móvil y un equipo externo tal como un puesto de conexión de pago.

45 De ese modo, es posible, con la ayuda del terminal móvil, efectuar un pago mediante comunicación sin contacto. Una comunicación de ese tipo está, por ejemplo, de acuerdo con la norma ISO 14 443 que concierne a un formato de tarjeta de identificación y a un protocolo de comunicación asociado.

50 Para utilizar este tipo de servicios o para intercambiar unas informaciones, el usuario aproxima su terminal móvil al puesto de conexión, de tal manera que se pueda realizar una transacción mediante comunicación en campo cercano.

55 Además, se puede activar una selección de aplicaciones bancarias en la tarjeta de identificación del terminal móvil utilizado, por ejemplo mediante el microcontrolador de una tarjeta SIM. La activación de esta selección de aplicaciones está controlada por ejemplo por el terminal móvil de acuerdo con la norma ISO 7816 relativa a las tarjetas de identificación de contactos. El usuario puede elegir entonces una de las aplicaciones bancarias seleccionadas.

60 Como se ha indicado anteriormente y con el fin de asegurar una operación efectuada mediante la aplicación elegida, se puede efectuar una autenticación del usuario. Ésta puede consistir particularmente en solicitar una palabra clave al usuario, por ejemplo su código PIN (acrónimo de *Personal Identification Number* en terminología anglosajona), a través de una interfaz gráfica del terminal móvil. El código PIN utilizado en este caso es generalmente diferente al código PIN utilizado para acceder a las funciones de telefonía. Después de que el usuario la haya introducido, por ejemplo con la ayuda del teclado, real o virtual (utilizando por ejemplo una pantalla táctil), esta palabra clave se transmite a la tarjeta de identificación, por ejemplo de acuerdo con la norma ISO 7816, que la compara con un código almacenado en una memoria no volátil de la tarjeta de identificación. Si esta palabra clave y este código coinciden, la operación se autoriza, en el caso contrario, se rechaza.

Por razones de seguridad, la palabra clave introducida por el usuario tiene generalmente una duración limitada. De ese modo, si la operación pretendida no se ha efectuado en el plazo fijado, el código expira. Un plazo de ese tipo está generalmente predeterminado, su valor es típicamente de un minuto. Si el plazo ha expirado y el usuario desea en cualquier caso efectuar la operación pretendida, debe reintroducir la palabra clave.

Aunque un sistema de ese tipo permite limitar los riesgos de fraude, existe en cualquier caso una necesidad constante de mejorar la seguridad ligada a la ejecución de ciertas operaciones efectuadas desde el terminal móvil, particularmente transacciones.

La invención permite resolver al menos uno de los problemas expuestos anteriormente.

La invención tiene ese modo por objetivo un procedimiento de control de la ejecución de al menos una función interna protegida integrada en un dispositivo de microcircuitos adaptado para ser utilizado en cooperación con un terminal móvil, este procedimiento, implementado en dicho dispositivo de microcircuitos, comprende las etapas siguientes:

- detección de una orden de puesta en suspensión de dicho dispositivo de microcircuitos, siendo detectada dicha orden de puesta en suspensión a partir de una información recibida desde un terminal móvil en el que está conectado dicho dispositivo de microcircuitos;

- análisis de al menos una indicación relativa a la ejecución de dicha al menos una función interna protegida; y

- si dicha al menos una función interna protegida es susceptible de ser afectada por la ejecución de dicha orden de puesta en suspensión, ejecución diferida de dicha orden de puesta en suspensión.

El procedimiento de acuerdo con la invención permite de ese modo proteger la integridad de un dispositivo de microcircuitos tal como una tarjeta de microcircuitos y asegurar la protección de aplicaciones protegidas ejecutadas por este dispositivo difiriendo, si es necesario, la ejecución de órdenes de puesta en suspensión del dispositivo. Con estos propósitos, se difiere una orden de puesta en suspensión en función de la ejecución de funciones internas protegidas, por ejemplo de funciones de descuento que pueden ser utilizadas para determinar la validez de una palabra clave o de funciones de gestión de memorias del dispositivo de microcircuitos.

Según un modo de realización particular, el procedimiento comprende además las etapas siguientes:

- la colocación a un primer valor de una variable de estado durante el lanzamiento de dicha al menos una función interna protegida, y

- la colocación a un segundo valor de dicha variable de estado cuando la ejecución de dicha al menos una función interna protegida se termina o cuando dicha función interna protegida de reinicializa;

comprendiendo dicha etapa de análisis una etapa de análisis del valor de dicha variable de estado.

Según este modo de realización, se utiliza una variable de estado como medio de intercambio de informaciones entre unas funciones internas protegidas y un módulo de gestión de puesta en suspensión del dispositivo, pudiendo este módulo, en función del valor de esta variable, es decir en función de la ejecución de las funciones internas protegidas, diferir o no la ejecución de una orden de puesta en suspensión.

Según otro modo de realización, la ejecución de dicha orden de puesta en suspensión está controlada directamente por dicha al menos una función interna protegida. No es necesario entonces utilizar una variable de estado con este propósito.

De manera ventajosa, el procedimiento comprende además una etapa de comparación de un nivel de suspensión solicitado asociado a dicha orden de puesta en suspensión, con un estado de suspensión de dicho dispositivo de microcircuitos. De ese modo, según los valores relativos de los niveles de suspensión solicitado y real, se puede determinar si es necesario o no verificar si la ejecución de una orden de puesta en suspensión debe ser diferida o no.

Siempre según un modo de realización particular, estando provisto dicho dispositivo de microcircuitos o dicho terminal móvil de medios de comunicación inalámbrica de alcance reducido y comprendiendo dicho dispositivo de microcircuitos una aplicación protegida integrada que hace llamada a dichos medios de comunicación inalámbrica de alcance reducido y a dicha función interna protegida, el procedimiento comprende además las etapas siguientes:

- recepción de un dato de autenticación para la ejecución de dicha aplicación protegida, siendo recibido dicho dato de autenticación desde dicho terminal móvil;

- comparación de dicho dato de autenticación recibido con al menos un dato almacenado en dicho dispositivo de microcircuitos;

5 - si dicho dato de autenticación recibido corresponde a dicho al menos un dato almacenado y si dicha aplicación protegida ha sido llamada, verificación de la validez de dicho dato de autenticación recibido según al menos un criterio definido dinámicamente en dicho dispositivo de microcircuitos; y

- si dicho dato de autenticación recibido es válido, ejecución de dicha aplicación protegida.

10 El procedimiento según la invención permite de ese modo determinar la validez de una palabra clave recogida por un usuario, sin recurrir a unos medios del terminal móvil en el que se utiliza el dispositivo de microcircuitos. El procedimiento según la invención permite de ese modo mejorar la seguridad ligada a la utilización de una palabra clave.

15 De manera ventajosa, dicha función interna protegida es una función de descuento, comprendiendo el procedimiento además, si dicho dato de autenticación recibido corresponde a dicho al menos un dato almacenado, una etapa de llamada a dicha función de descuento para un plazo de una duración predeterminada, comprendiendo dicha etapa de verificación la verificación de que dicho plazo no ha expirado. La validez de una palabra clave está de ese modo limitada en el tiempo, siendo efectuado el descuento del tiempo de manera segura en el dispositivo de microcircuitos. Dicha función de descuento está, preferiblemente, basada en un reloj material de dicho dispositivo de microcircuitos.

Siempre según un modo de realización particular, el procedimiento comprende además las etapas siguientes:

25 - recepción de al menos una información de dicho terminal móvil al que está conectado dicho dispositivo de microcircuitos para informar que al menos un puesto de conexión de acceso sin contacto está accesible a través de dichos medios de comunicación inalámbricos de alcance reducido;

30 - selección de al menos dicha aplicación protegida integrada en dicho dispositivo de microcircuitos en respuesta a dicha al menos una información recibida, y transmisión de al menos una referencia a dicha al menos una aplicación seleccionada a dicho terminal móvil; y

- recepción de al menos un identificador de una aplicación, correspondiendo dicho identificador a una referencia a dicha aplicación protegida integrada.

35 El procedimiento permite de ese modo la implementación simple y segura de aplicaciones tales como unas aplicaciones de pago.

40 La invención tiene igualmente por objetivo un programa de ordenador que comprende unas instrucciones adaptadas para la implementación de cada una de las etapas del procedimiento descrito anteriormente cuando dicho programa se ejecuta en un ordenador.

45 La invención tiene también por objetivo un dispositivo que comprende unos medios, tales como un microcontrolador, adaptados para la implementación de cada una de las etapas del procedimiento descrito anteriormente así como una tarjeta de identificación de un abonado en una red de telefonía móvil que comprende un dispositivo de este tipo y un terminal móvil que integra un dispositivo de este tipo.

50 Según un modo de realización particular, el dispositivo comprende además al menos una memoria configurada para memorizar al menos un dato relativo a dicha al menos una función integrada protegida. Siempre según un modo de realización particular, el microcontrolador está configurado además para ejecutar un algoritmo de criptografía que protege dicho al menos un dato relativo a dicha al menos una función interna protegida y/o para ejecutar un algoritmo de protección material de al menos un componente de dicho dispositivo con el fin de mejorar la protección de dicha al menos una función interna.

55 Las ventajas proporcionadas por este programa de ordenador, este dispositivo y esta tarjeta de identificación son similares a las evocadas anteriormente.

60 Surgirán otras ventajas, objetivos y características de la presente invención con la descripción detallada a continuación, realizada a título de ejemplo no limitativo, en relación a unos dibujos adjuntos en los que:

- la figura 1 representa esquemáticamente un terminal móvil y una tarjeta de microcircuitos asociada que permiten la realización de la invención;

- la figura 2 ilustra ciertas etapas realizadas en un terminal móvil de acuerdo con la invención;

65 - la figura 3 ilustra ciertas etapas realizadas en una tarjeta de microcircuitos de acuerdo con la invención; y

- la figura 4 ilustra ciertas etapas de un ejemplo de algoritmo del módulo de gestión de puesta en suspensión, de acuerdo con la invención.

5 Se ha observado que la seguridad ligada a la ejecución de ciertas operaciones efectuadas por un terminal móvil en conjunto con una tarjeta de microcircuitos presenta unas debilidades porque una parte del mecanismo de seguridad se realiza en el terminal móvil y porque este último no se puede considerar como una zona de ejecución segura.

10 En particular, se ha observado que en razón de las especificaciones de los operadores móviles y bancarios, los terminales móviles realizan unas aplicaciones intermediarias. Estas últimas se utilizan particularmente para calcular el plazo de expiración de una palabra clave introducida por un usuario. Éstas se pueden implementar bajo forma de *midlet*, es decir un conjunto de API (sigla de *Application Program Interface* en terminología anglosajona) Java que define la manera con la que unas aplicaciones ejecutadas en una tarjeta insertada en un terminal móvil se conectan a la interfaz del terminal. Igualmente, una palabra clave puede ser válida para un número de utilizations dado.

15 En otros términos, unas aplicaciones protegidas que deben ser ejecutadas por medio de un terminal móvil tienen una seguridad relativa. A título de ilustración, la orden de invalidación de la palabra de clave como resultado de un plazo de expiración es una función implementada en un terminal móvil y cuyo resultado se transmite típicamente de manera no segura a una tarjeta de microcircuitos, por ejemplo una tarjeta SIM. Los midlets que realizan estas funciones no están certificados, particularmente por unas autoridades bancarias. Estas funciones pueden ser por lo tanto el objetivo de los ataques fraudulentos y sus resultados pueden ser interceptados.

20 Además, unos midlets pueden fallar lo que puede conducir a que una palabra clave sea válida durante un periodo importante. De ese modo, por ejemplo, cuando un usuario debe introducir una palabra clave para efectuar las transacciones superiores a una suma dada, puede efectuar unas transacciones superiores a esta suma sin darse cuenta de si el mecanismo de expiración de la palabra clave está fallando.

30 Por otro lado, se observa que las tarjetas de microcircuitos están provistas generalmente de un modo, denominado modo de suspensión, que permite inhibir, parcial o totalmente, unas funciones de esas tarjetas. Un modo de ese tipo tiene por objetivo reducir el consumo eléctrico de la tarjeta de microcircuitos con el fin de preservar la carga de la batería del terminal móvil en el que se utiliza la tarjeta de microcircuitos (estando típicamente alimentada una tarjeta de microcircuitos por el terminal móvil al que está conectada). De ese modo, en otros términos, existe un estado activo en el que una tarjeta de microcircuitos puede utilizarse "normalmente", uno o varios estados de suspensión según los cuales sólo ciertas funciones de la tarjeta se pueden utilizar y un estado de parada en el que no se puede utilizar ninguna función. Para pasar a un estado activo o de suspensión a partir del estado de parada, es necesario generalmente arrancar la tarjeta, lo que toma un tiempo generalmente no despreciable. El estado de la tarjeta de microcircuitos está, según las normas actuales, controlado por el terminal móvil en el que se utiliza la tarjeta. De ese modo, por ejemplo, la función del terminal móvil para poner en suspensión una tarjeta de microcircuitos, más precisamente para detener su reloj interno es, según la norma ISO 7816 "*clockstop*" que tiene por efecto detener la señal de reloj transmitida por el terminal móvil a la tarjeta de microcircuitos. Cuando la tarjeta de microcircuitos detecta la detención de la señal de reloj, se pone en suspensión.

45 La invención se dirige a la realización de funciones internas protegidas, particularmente funciones de seguridad, por ejemplo unas funciones de cálculo de un plazo de expiración de una palabra clave o, más generalmente, de un dato de autenticación introducido por un usuario, en una tarjeta de microcircuitos, por ejemplo una tarjeta SIM, UICC, UMTS o RUIM, configurada para ser utilizada en cooperación con un terminal móvil. De ese modo, de acuerdo con la invención, la validación de un dato de autenticación del usuario se efectúa según un criterio definido dinámicamente en la tarjeta de identificación. Este criterio es típicamente una duración de la validez y/o un número de utilizations. La invención se dirige igualmente a la realización de otras funciones protegidas tales como unas funciones de gestión de memoria.

50 La figura 1 representa un terminal móvil 100 adecuado para la realización de la invención. Como se ilustra, el terminal móvil 100 comprende un módulo 105 de telefonía móvil, ventajosamente conectado a un altavoz 110 y a un micrófono 115. El módulo de telefonía móvil está conectado a una antena (no representada) del terminal móvil 100 para comunicar con la red de telefonía móvil. El terminal móvil 100 comprende igualmente una unidad central de procesamiento 120, también denominada CPU (sigla de *Central Processing Unit* en terminología anglosajona) y, preferiblemente, una pantalla 125.

60 El terminal móvil 100 comprende además un módulo 130 de comunicación de alcance reducido, ventajosamente un módulo de comunicación inalámbrica de alcance reducido. El módulo 130 es por ejemplo del tipo NFC. El módulo 130 puede estar directamente implantado en el terminal móvil 100, por ejemplo en la forma de un circuito integrado y de antena, o insertado en el terminal móvil 100, por ejemplo, en la forma de una tarjeta de microcircuitos que comprende una antena integrada.

65 El terminal móvil comprende igualmente un dispositivo de entrada 135, tal como un teclado o un dispositivo equivalente, para introducir unos caracteres, unos valores y/o unas órdenes. El dispositivo de entrada 135 forma, en

cooperación con la pantalla 125, una interfaz de usuario. El dispositivo de entrada 135 puede estar igualmente integrado en la pantalla 125 bajo la forma de una pantalla táctil.

El terminal móvil 100 comprende también un módulo de memoria 140 adaptado para memorizar al menos unas aplicaciones y/o unas interfaces de programas 145 utilizadas entre el terminal móvil 100 y ciertos de estos componentes, fijos o extraíbles, tales como el módulo 130 y una tarjeta de microcircuitos conectada a este terminal móvil, por ejemplo la tarjeta de identificación 150.

La tarjeta de identificación 150 es en este caso una tarjeta SIM provista con un microcontrolador 155, una primera memoria 160 y una segunda memoria 170. La primera memoria 160 se utiliza en este caso para almacenar unas aplicaciones tales como unas aplicaciones de usuario, de su operador y unas aplicaciones bancarias. Una parte 165 de esta memoria se utiliza además para almacenar unas informaciones, unos parámetros y/o unas informaciones del usuario para permitirle acceder a una red de telefonía móvil, en particular un código del tipo PIN. La primera memoria 160 es típicamente memoria del tipo flash. La segunda memoria 170 es en este caso una memoria del tipo ROM (acrónimo de *Read Only Memory* en terminología anglosajona). Se utiliza particularmente para almacenar el sistema operativo de la tarjeta de identificación así como unas funciones de interfaz.

Según un modo de realización particular, el módulo 130 de comunicación de alcance reducido puede estar integrado, total o parcialmente, en la tarjeta de identificación 150.

La tarjeta de identificación 150 es, preferiblemente, extraíble y segura.

La invención se dirige a un mecanismo realizado directamente en una tarjeta de microcircuitos, es decir, de manera general, un dispositivo de microcircuitos, por ejemplo en la tarjeta SIM 150, para controlar la ejecución de funciones internas protegidas, en relación al estado de la tarjeta, particularmente funciones internas llamadas por las aplicaciones protegidas. El dispositivo de microcircuitos, que comprende por ejemplo el microcontrolador 155 y las memorias 160 y 170, puede estar integrado en el terminal móvil.

Según un modo de realización particular, la invención tiene por objetivo un mecanismo para generar dinámicamente la validez de una palabra clave introducida por un usuario con ayuda de medios de entrada tales como el teclado 135. Este mecanismo puede consistir particularmente en controlar la duración de la validez de la palabra clave y/o para comprobar el número de ejecuciones de una aplicación protegida utilizando una misma palabra clave introducida. Un mecanismo interno de ese tipo en la tarjeta de microcircuitos es menos sensible a los ataques que un mecanismo similar realizado en un terminal móvil porque el entorno de una tarjeta de microcircuitos es generalmente más seguro que el entorno del terminal móvil. Además, un mecanismo de ese tipo puede ser certificado más fácilmente, por ejemplo por una autoridad bancaria.

De manera ventajosa, este mecanismo utiliza una función interna de la tarjeta de microcircuitos, generalmente denominada *timer* en terminología anglosajona. Un *timer* se define típicamente como una función, material o por programa, encargada de generar una interrupción después de un número de impulsos de reloj para activar o ejecutar otra función, típicamente del código del programa. Este número de impulsos de reloj y el reloj que debe utilizarse (por ejemplo el reloj de la tarjeta de microcircuitos) están generalmente proporcionados en la función como parámetros.

De acuerdo con la invención, se añade una interfaz (API), por ejemplo, al sistema operativo utilizado en el seno de la tarjeta de microcircuitos para ofrecer unas funciones internas de control de la validez de una palabra clave recibida desde el terminal móvil al que está conectada la tarjeta. Estas funciones permiten particularmente descontar una duración predefinida de la validez de la palabra clave. La interfaz añadida consiste en este caso por ejemplo en un servicio suministrado por el sistema operativo de la tarjeta SIM, en una aplicación bancaria, por ejemplo una aplicación del tipo *cardlet*. Un servicio de ese tipo se llama por ejemplo cuando una palabra clave recibida se considera como correcta, es decir cuando corresponde a un dato de autenticación previamente memorizado.

Para controlar una duración predefinida de validez de la palabra clave, se utiliza preferiblemente el reloj material de la tarjeta de microcircuitos. La función *timer* que utiliza un reloj de ese tipo, también denominada *hardware timer* en terminología anglosajona, se puede considerar como una extensión material del sistema operativo de la tarjeta de microcircuitos, siendo generalmente el sistema operativo un programa. Esta función de *hardware timer*, existente generalmente en el seno de las tarjetas SIM, más precisamente en el seno del microcontrolador, ofrece la ventaja de estar normalmente certificado por los fabricantes, de acuerdo con los criterios comunes conocidos bajo nombre de EAL4+.

Como variante, se puede utilizar una variante de *timer* por programa (denominada *software timer* en terminología anglosajona). El reloj utilizado con estos propósitos puede estar generado al partir del reloj material de la tarjeta de microcircuitos o a partir de un reloj del terminal móvil. Una función *timer* por programa no está generalmente certificada por los fabricantes.

De acuerdo con un modo de realización preferido, la tarjeta de microcircuitos comprende al menos dos niveles de

suspensión. Un primer nivel corresponde a una suspensión total según la que el conjunto de los componentes están en suspensión (se trata por lo tanto de un modo de suspensión estándar). Un segundo nivel corresponde a una suspensión parcial según en la que ciertas funciones están activas. De ese modo, por ejemplo, la función de descuento de una duración predefinida de la validez de una palabra clave puede permanecer activa en este nivel de suspensión. En otros términos, en este modo de suspensión parcial, la función *timer* (*software timer* o *hardware timer*) está en este caso activa.

La figura 2 ilustra ciertas etapas realizadas en un terminal móvil de acuerdo con la invención.

Una primera etapa (etapa 200) tiene por objetivo la detección de un puesto de conexión, por ejemplo un puesto de conexión de pago de un objeto o de un servicio, tal como el acceso a un museo. Según la configuración del módulo de comunicación inalámbrico de alcance reducido utilizado, esta etapa puede realizarse automáticamente por la detección de una señal o en respuesta a una orden del usuario realizada por medio de una interfaz del terminal móvil utilizado.

En una etapa siguiente (etapa 205), se establece un canal de comunicación entre el terminal móvil y el puesto de conexión previamente detectado. Este canal de comunicación se establece en este caso según un protocolo estándar, por ejemplo un protocolo de acuerdo con la norma ISO 14 443. Paralelamente, de manera simultánea o previamente, se establece un canal de comunicación entre el terminal móvil utilizado y la tarjeta de microcircuitos contenida en este último (etapa 210). De nuevo, este canal de comunicación se establece preferentemente según un protocolo estándar, por ejemplo, un protocolo de acuerdo con la norma ISO 7816.

A continuación, se transmite una información relativa al puesto de conexión detectado, a la tarjeta de microcircuitos para permitirle seleccionar unas aplicaciones contenidas en esta última y que pueden ser ejecutadas. La selección de aplicaciones se basa, preferiblemente, en el tipo de puesto de conexión detectado. Una referencia a estas aplicaciones seleccionadas se transmite al terminal móvil, por ejemplo en la forma de lista (etapa 215). Se trata, por ejemplo, de aplicaciones bancarias.

La lista de las aplicaciones seleccionadas puede presentarse sobre el terminal móvil con el fin de permitir al usuario elegir una (etapa 220). Se transmite entonces una referencia de la aplicación elegida a la tarjeta de microcircuitos que, llegado el caso, indica al terminal móvil que debe introducir una palabra clave por parte del usuario. En este caso, el usuario introduce una palabra clave con la ayuda, por ejemplo, de un teclado o de un dispositivo similar ligado al terminal móvil (etapa 225). Esta palabra clave se transmite entonces a la tarjeta de microcircuitos, por ejemplo según la norma ISO 7816, que la verifica y lanza la ejecución de la aplicación elegida, es decir de las funciones de esta aplicación. Esas funciones pueden ser identificadas por la aplicación elegida por sí misma o ser seleccionadas por el usuario. Puede tratarse particularmente de una orden de pago cuyo montante puede ser introducido por el usuario o transmitido por el puesto de conexión durante el establecimiento de la comunicación entre el terminal móvil y el puesto de conexión.

Durante la ejecución de estas funciones (etapa 230), se requiere generalmente al terminal móvil como interfaz entre la tarjeta de microcircuitos y el módulo de comunicación inalámbrico de alcance reducido del terminal móvil.

Como se ha ilustrado, el procedimiento se puede repetir mientras que no se le haya puesto fin (de manera automática o por el usuario).

La figura 3 ilustra ciertas etapas realizadas en una tarjeta de microcircuitos, por ejemplo una tarjeta SIM, de acuerdo con la invención.

Una primera etapa (etapa 300) se dirige en este caso a la selección de las aplicaciones contenidas en la tarjeta de identificación. Como se ha descrito anteriormente, una selección de ese tipo se efectúa, preferiblemente, según las características de un puesto de conexión, con el que el terminal móvil que comprende la tarjeta de microcircuitos, ha establecido un canal de comunicación. Dichas características pueden de ese modo dirigirse a unas indicaciones relativas al pago de una suma o a la recarga de un monedero electrónico o de un abono de comunicación.

Se transmiten entonces al terminal móvil unas referencias a las aplicaciones seleccionadas, por ejemplo en forma de una lista. Cuando dicha lista se recibe por parte el terminal móvil, se presentan preferiblemente de manera que el usuario pueda elegir una. Cuando ha sido elegida una aplicación, se transmite a la tarjeta de microcircuitos una referencia a ésta, más precisamente al microcontrolador de la tarjeta de microcircuitos, para permitirle lanzar la aplicación correspondiente (etapa 305).

Alternativamente, si una única aplicación es susceptible de ser ejecutada o en función de parámetros de configuración, puede lanzarse directamente una aplicación sin que haya sido elegida explícitamente por el usuario.

Durante el lanzamiento de la aplicación, se efectúa una prueba para determinar si la aplicación está protegida, es decir si la ejecución de esta aplicación o de ciertas de sus funciones requieren la autenticación del usuario (etapa 310). En caso negativo, la aplicación se ejecuta de manera clásica por el microcontrolador de la tarjeta de

microcircuitos.

En caso contrario, si la aplicación está protegida, se transmite en este caso una instrucción al terminal móvil con el fin de obtener una palabra clave que permita desbloquear la aplicación mediante la autenticación. Esta última se introduce, preferiblemente, por el usuario, con la ayuda de un teclado o de un dispositivo similar ligado al terminal móvil y después se transmite a la tarjeta de microcircuitos.

Se ha observado en este caso que unos datos ligados a la o a las funciones protegidas, memorizadas en unas memorias de la tarjeta de microcircuitos, por ejemplo en la memoria 160 y/o la memoria 170 descritas con referencia a la figura 1, pueden estar protegidas con la ayuda de algoritmos de criptografía que respetan la norma FIPS (acrónimo de *Federal Information Processing Standards* en terminología anglosajona).

De manera similar, unos componentes de la tarjeta de microcircuitos tales como el microcontrolador 155 y las memorias 160 y 170 descritas con referencia a la figura 1, en las que están memorizados unos datos relativos a la o a las funciones protegidas, pueden estar protegidos materialmente contra unos ataques denominados no invasivos (por ejemplo unos ataques mediante análisis de tiempos, análisis de consumo, análisis electromagnético y/o ataques de relojes), invasivos o semi-invasivos.

Después de haber obtenido la palabra clave (etapa 315), se efectúa una prueba para determinar si la palabra clave recibida es correcta (etapa 320). Con estos fines, el microcontrolador de la tarjeta de microcircuitos, o un módulo criptográfico ligado a este microcontrolador, compara la palabra clave recibida con un dato previamente memorizado, una comparación de este tipo puede realizarse particularmente según unos algoritmos de autenticación y de criptografía estándar.

Alternativamente, se pueden utilizar otros modos de autenticación tales como el reconocimiento de huellas digitales.

Si la palabra clave no era correcta, esto pone fin al proceso o se transmite una instrucción al terminal móvil para invitar al usuario a reintroducir una palabra clave (como se indica por la utilización de una flecha en trazo de puntos).

Por el contrario, si la palabra clave es correcta, se activa una función de descuento del tiempo (es decir una función interna protegida (etapa 325). Como se ha descrito anteriormente, esta función tiene por objetivo identificar un intervalo de tiempo en el que la palabra clave recibida se considera como válida. La duración de este intervalo de tiempo está, preferiblemente, predeterminada. La función de descuento se basa en un reloj de la tarjeta de microcircuitos o, alternativamente, en un reloj del terminal móvil.

Alternativamente, la función de descuento puede lanzarse antes de verificar la palabra clave, siendo detenida la función de descuento si la palabra clave no es correcta.

La función de descuento se basa típicamente en la función *timer* (preferiblemente la función *hardware timer*) descrita anteriormente. Esta última se llama con, como parámetros, la duración de validez de la palabra clave y el reloj que debe utilizarse. Con la expiración del *timer*, es decir al final de la ejecución de la función *timer*, se genera una interrupción. Ésta indica a la función de descuento que se ha terminado. La función de descuento puede asimilarse igualmente a la función *timer*.

Según un modo de realización particular, se transmite una primera indicación al sistema operativo de la tarjeta de microcircuitos, o más generalmente a un módulo de gestión de puesta en suspensión, cuando se activa la función de descuento. Igualmente, se transmite una segunda indicación al sistema operativo de la tarjeta de identificación, o más generalmente a un módulo de gestión de la puesta en suspensión, cuando la función de descuento se reinicializa o se termina el descuento. De ese modo, conociendo el estado de la función de descuento, el sistema operativo, o más generalmente un módulo de gestión de puesta en suspensión, pueden impedir el estado de suspensión total de la tarjeta de identificación cuando la función de descuento está activa. En otros términos, sólo puede utilizarse un estado activo o un estado de suspensión parcial según el que el reloj de la tarjeta de microcircuitos está activo, cuando la función de descuento está activa (cuando se utiliza el reloj de la tarjeta de identificación). Si la función de descuento se basa en un reloj del terminal móvil, el estado de suspensión parcial es un estado según el que la función de descuento es operativa sin que el reloj de la tarjeta de identificación esté necesariamente activo.

Alternativamente, se puede impedir cambiar el estado de la tarjeta de identificación cuando la función de descuento está activa. De este modo, de manera ventajosa, se pone una variable de estado, preferiblemente memorizada en una memoria volátil, por ejemplo la variable de estado *PIN_OK*, en un primer valor cuando la función de descuento está activa (por ejemplo, *PIN_OK*=1). Esta variable de estado se pone a un segundo valor cuando la función de descuento se reinicializa o cuando el descuento ha finalizado (por ejemplo, *PIN_OK*=0). Alternativamente esta variable de estado puede ponerse directamente en este segundo valor cuando la función *timer* emite una interrupción (cuando expira el *timer*), siendo entonces desactivada la función de descuento cuando la variable de estado se pone en este segundo valor. En este caso, la interrupción generada por la función *timer* desencadena la

función, preferiblemente por programa, de puesta al día de la variable de estado *PIN_OK*.

A continuación, cuando se trata por el microcontrolador de la tarjeta de microcircuitos una orden dirigida a la ejecución de una función de la aplicación protegida, se efectúa una prueba para determinar si la palabra clave recibida es válida (etapa 335). Se observa en este caso que una orden dirigida a la ejecución de una función de la aplicación protegida puede estar directamente ligada a esta última (ésta, en este caso, se recibe automáticamente) puede ser el resultado de una elección del usuario (la orden se recibe entonces a través de la unidad central de tratamiento 120 por medio de una instrucción que sale del terminal móvil, como se ilustra por la flecha en trazo de puntos) o puede provenir del puesto de conexión al que está conectado el terminal móvil (la orden se recibe entonces a través del módulo 130, como se ilustra por la flecha en trazo de puntos).

Para determinar si una palabra clave es válida, el microcontrolador de la tarjeta de microcircuitos llama en este caso a la función de descuento del tiempo lanzada anteriormente. De ese modo, si el plazo ha expirado, la palabra clave se considera como no válida. Además, según un modo de realización particular, el número de ejecuciones de la aplicación protegida (o de funciones de esta aplicación) desde la introducción de la palabra clave se puede comparar con un número de utilizaciones predeterminado. Es posible de este modo limitar la utilización de la palabra clave a una única orden, dos órdenes, etc.

Si la palabra clave no es válida, se transmite una instrucción al terminal móvil para invitar al usuario a reintroducir una palabra clave (el algoritmo vuelve a la etapa 315 descrita anteriormente).

Si, por el contrario, se considera la palabra clave como válida, la orden considerada se trata y la función correspondiente se ejecuta (etapa 340). Como se ha indicado anteriormente, la ejecución de esta función puede hacer llamada al terminal móvil, particularmente para requerir el modo de comunicación inalámbrica de alcance reducido utilizado. Según un modo de realización particular, según el que no se puede utilizar una palabra clave más que para la ejecución de una única función, la función de descuento del tiempo se reinicializa (para detenerla). De esa manera, si se debe ejecutar una nueva orden protegida, la palabra clave será considerada como no válida sin que sea necesario comparar el número de órdenes ejecutadas desde la recepción de esta palabra clave con un número de utilizaciones predeterminado.

Se observa en este caso que unas aplicaciones pueden estar protegidas porque la ejecución de ciertas de sus funciones está sometida a ciertas limitaciones, particularmente a la autenticación del usuario, como se ha descrito anteriormente. Sin embargo, una aplicación puede estar igualmente protegida de manera global, es decir que cuando la ejecución de la aplicación ha sido autorizada (después de la autenticación del usuario), no hay necesidad de autenticar al usuario para ejecutar sus funciones. En cualquier caso, cuando esta aplicación hace llamada a otra aplicación protegida, puede ser necesario volver a autenticar al usuario para ejecutar esta otra aplicación.

Cuando la tarjeta de microcircuitos detecta una orden de puesta en suspensión y si el nivel de puesta en suspensión es tal que es susceptible de afectar a la ejecución de la aplicación protegida, particularmente la función interna de descuento, se efectúa una prueba para determinar si la orden de puesta en suspensión puede ser ejecutada o si su ejecución debe ser diferida. Con estos propósitos, se realiza un módulo de gestión de la puesta en suspensión, preferiblemente, en la tarjeta de microcircuitos. Se puede tratar de un módulo material o de un módulo por programa. Puede particularmente estar integrado en el sistema operativo de la tarjeta de microcircuitos. Si se utiliza una variable de estado, por ejemplo la variable de estado *PIN_OK*, memorizada preferiblemente en la memoria volátil, el módulo de gestión de puesta en suspensión determina el valor de la variable de estado y, en función de este valor, autoriza o no la puesta en estado de suspensión solicitada.

La figura 4 ilustra ciertas etapas de un ejemplo de algoritmo de un módulo de gestión de puesta en suspensión, de acuerdo con la invención. Como se ilustra, una primera etapa (etapa 400) tiene por objetivo la detección de una orden de puesta en suspensión de la tarjeta de microcircuitos que comprende este módulo. De acuerdo con la norma ISO 7816, esta orden se detecta a partir de la señal de reloj que proviene del sistema móvil en el que se utiliza la tarjeta de microcircuitos, cuando la señal de reloj se detiene.

En una etapa siguiente, el módulo de gestión de puesta en suspensión determina si el estado de suspensión solicitado, asociado a la orden de puesta en suspensión, es inferior al estado de suspensión actual (etapa 405), es decir si el estado de suspensión solicitado requiere la activación de ciertas funciones de la tarjeta de microcircuitos (el estado de suspensión solicitado es, en este caso, inferior o igual al estado de suspensión actual) o si, por el contrario, el estado de suspensión solicitado requiere la inhibición de ciertas funciones de la tarjeta de microcircuitos (el estado de suspensión es, en este caso superior al estado de suspensión actual).

Si el estado de suspensión solicitado es inferior o igual al estado de suspensión actual, la orden de puesta en suspensión recibida se ejecuta (etapa 410).

Por el contrario, si el estado de suspensión solicitado es superior al estado de suspensión actual, se efectúa una prueba para determinar el valor de la variable de suspensión utilizada para indicar que unas funciones internas protegidas son susceptibles de ser afectadas por una puesta en suspensión de nivel superior al estado de

suspensión actual (etapa 415). Según un ejemplo dado anteriormente, esta etapa requiere en este caso determinar el valor de la variable de estado *PIN_OK*.

- 5 Si el valor de la variable de estado utilizada indica que unas funciones internas protegidas no son susceptibles de ser afectadas por una puesta en suspensión de un nivel superior al estado de suspensión actual, la orden de puesta en suspensión recibida se ejecuta (etapa 410).

- 10 Por el contrario, si el valor de la variable de estado utilizada indica que unas funciones internas protegidas son susceptibles de ser afectadas por una puesta en suspensión de un nivel superior al estado de suspensión actual, se efectúa otra prueba para determinar si el nivel de suspensión solicitado afecta a la ejecución de la función interna protegida (etapa 420). Por ejemplo si el estado de suspensión solicitado tiene por objetivo inhibir la función de descuento o la función *timer* (si son diferentes). En caso afirmativo, se repiten las dos últimas etapas (etapas 415 y 420) para diferir la ejecución de la orden de puesta en suspensión detectada.

- 15 Como variante, puede utilizarse la interrupción generada por la función *timer* para desencadenar una función, preferiblemente por programa, de puesta al día de la variable de estado *PIN_OK*, esta función de puesta al día comprende una función de gestión de la suspensión. De ese modo, si se ha detectado previamente una orden de puesta en suspensión, es decir si una suspensión está en espera, la tarjeta de microcircuitos se pone en suspensión durante esta interrupción, a continuación de una puesta al día de la variable de estado *PIN_OK*.

- 20 Por el contrario, si el nivel de suspensión solicitado no afecta a la ejecución de la función interna protegida, la orden de puesta en suspensión detectada se ejecuta (etapa 410).

- 25 El valor de la variable de estado utilizada se puede memorizar en una memoria volátil o no volátil según los niveles de suspensión de las tarjetas de microcircuitos de tal manera que este valor sea accesible en el estado de suspensión más elevado de acuerdo con el que una función interna protegida se puede ejecutar. Se observa en este caso que puede ser posible modificar el estado de suspensión (pasar a un estado de suspensión de un nivel inferior) para cambiar el valor de una variable de estado.

- 30 Según un modo de realización particular, la ejecución de las órdenes de puesta en suspensión se puede controlar por las funciones internas protegidas que generan las variables de estado relativas a estas últimas o mediante las aplicaciones protegidas que hacen llamada a estas funciones internas protegidas. Según este modo de realización, las funciones internas protegidas o las aplicaciones protegidas, después de haber recibido una indicación según la que ha sido detectada una orden de puesta en suspensión, indican al módulo de gestión de puesta en suspensión el
35 instante en el que las órdenes de puesta en suspensión se pueden ejecutar.

- Según otro modo de realización, una función interna protegida integrada en una tarjeta de microcircuitos se relaciona con una función de gestión de la memoria de la tarjeta. Puede tratarse particularmente de una función denominada
40 "*wear leveling*".

- Se recuerda aquí que las memorias utilizadas en las tarjetas de microcircuitos comprenden generalmente unas memorias del tipo EEPROM (sigla de *Electrically-Erasable Programmable Read-Only Memory* en terminología anglosajona) que tienen típicamente un número limitado de ciclos de escritura, por ejemplo 20 ó 100 millones de escrituras, o, ciertas zonas de las memorias son accedidas generalmente, en escritura, más frecuentemente que
45 otras. De este modo, para evitar una caducidad prematura de una tarjeta de microcircuitos (ligada a la imposibilidad de escribir en ciertas zonas de memoria), se realiza la función de desplazamiento de los datos entre zonas de memoria con el fin de repartir también uniformemente, tanto como sea posible, las operaciones de escritura. Esta función de gestión de la memoria se denomina comúnmente *wear leveling*.

- 50 Una función interna de ese tipo se puede realizar paralelamente a la ejecución de aplicaciones llamadas por un usuario, pudiendo conducir a una reducción del rendimiento de las tarjetas de microcircuitos. Puede realizarse igualmente cuando las tarjetas de microcircuitos están inutilizadas. En este caso, la puesta en suspensión posterior de ciertos componentes de las tarjetas de microcircuitos, particularmente de los componentes a cargo de las operaciones de lectura y escritura, puede conducir, por ejemplo, a pérdidas de datos. Es necesario por lo tanto
55 prever un mecanismo de prevención de pérdidas de datos en caso de puesta en suspensión de las tarjetas de microcircuitos.

- Este problema se resuelve ventajosamente por la invención. Según un modo de realización particular, se transmite una primera indicación al sistema operativo de la tarjeta de identificación, o más generalmente a un módulo de
60 gestión de puesta en suspensión, cuando la función de *wear leveling* está activada. Igualmente, se transmite una segunda indicación al sistema operativo de la tarjeta de identificación, o más generalmente al módulo de gestión de puesta en suspensión, cuando la ejecución de la función de *wear leveling* ha finalizado. De ese modo, conociendo el estado de la función de *wear leveling*, el sistema operativo, o más generalmente un módulo de gestión de la puesta en suspensión, puede impedir el estado de suspensión total de la tarjeta de microcircuitos cuando la función de *wear
65 leveling* está activa. Alternativamente, se puede impedir cambiar el estado de la tarjeta de microcircuitos cuando la función de *wear leveling* está activa. Con estos fines, se pone una variable de estado, por ejemplo la variable de

estado *WL_OK*, en un primer valor cuando la función de *wear leveling* está activa (por ejemplo, *WL_OK*=1). Esta variable de estado se pone en un segundo valor cuando la función de *wear leveling* ha finalizado (por ejemplo, *WL_OK*=0).

- 5 El módulo de gestión de puesta en suspensión es similar entonces al descrito con referencia a la figura 4, siendo sustituida la variable de estado *PIN_OK* por la variable de estado *WL_OK*. De manera ventajosa, se puede utilizar una misma variable de estado, por ejemplo *SUSPENSIÓN_OK*, para controlar la ejecución de funciones internas protegidas con el fin de que sean diferidas unas órdenes de puesta en suspensión, llegado el caso.
- 10 Como se ha descrito anteriormente, los algoritmos descritos anteriormente, particularmente los algoritmos descritos con referencia a las figuras 3 y 4, se realizan ventajosamente en una tarjeta de microcircuitos, por ejemplo una tarjeta de identificación de abonado en una red de telefonía móvil, como una tarjeta SIM.
- 15 Naturalmente, para satisfacer necesidades específicas, una persona experta en la materia de la invención podrá aplicar modificaciones a la descripción precedente.

REIVINDICACIONES

1. Procedimiento de control de ejecución de al menos una función interna protegida integrada en un dispositivo de microcircuitos (150) adaptado para ser utilizado en cooperación con un terminal móvil (100), estando este
5 procedimiento caracterizado porque se realiza en dicho dispositivo de microcircuitos y porque comprende las etapas siguientes:
 - detección (400) de una orden de puesta en suspensión de dicho dispositivo de microcircuitos, siendo detectada
10 dicha orden de puesta en suspensión a partir de una información recibida desde un terminal móvil en el que está conectado dicho dispositivo de microcircuitos;
 - análisis (415) de al menos una indicación relativa a la ejecución de dicha al menos una función interna protegida; y
 - si dicha al menos una función interna protegida es susceptible de ser afectada por la ejecución de dicha orden de
15 puesta en suspensión, ejecución (410) diferida de dicha orden de puesta en suspensión.
2. Procedimiento según la reivindicación 1, que comprende además las etapas siguientes:
 - la colocación a un primer valor (325) de una variable de estado durante el lanzamiento de dicha al menos una
20 función interna protegida, y
 - la colocación a un segundo valor (325) de dicha variable de estado cuando la ejecución de dicha al menos una función interna protegida se termina o cuando dicha función interna protegida de reinicializa;
 - 25 comprendiendo dicha etapa de análisis una etapa de análisis del valor de dicha variable de estado.
3. Procedimiento según la reivindicación 1, según el cual dicha orden de puesta en suspensión está controlada por dicha al menos una función interna protegida.
- 30 4. Procedimiento según una cualquiera de las reivindicaciones 1 a 3, que comprende además una etapa de comparación (405) de un nivel de suspensión solicitado asociado a dicha orden de puesta en suspensión, con un estado de suspensión de dicho dispositivo de microcircuitos.
- 35 5. Procedimiento según una cualquiera de las reivindicaciones 1 a 4, estando provisto dicho dispositivo de microcircuitos o dicho terminal móvil de medios de comunicación inalámbrica de alcance reducido (130), comprendiendo dicho dispositivo de microcircuitos una aplicación protegida integrada que hace llamada a dichos medios de comunicación inalámbrica de alcance reducido y a dicha función interna protegida, comprendiendo además el procedimiento las etapas siguientes:
 - 40 - recepción (315) de un dato de autenticación para la ejecución de dicha aplicación protegida, siendo recibido dicho dato de autenticación desde dicho terminal móvil;
 - comparación (320) de dicho dato de autenticación recibido con al menos un dato almacenado en dicho dispositivo
45 de microcircuitos;
 - si dicho dato de autenticación recibido corresponde a dicho al menos un dato almacenado y si se llama a dicha aplicación protegida, verificación (335) de la validez de dicho dato de autenticación recibido según al menos un criterio definido dinámicamente en dicho dispositivo de microcircuitos; y
 - 50 - si dicho dato de autenticación recibido es válido, ejecución (340) de dicha aplicación protegida.
6. Procedimiento según la reivindicación 5, según el cual dicha función interna protegida es una función de descuento, comprendiendo el procedimiento además, si dicho dato de autenticación recibido corresponde a dicho al
55 menos un dato almacenado, una etapa de llamada (325) a dicha función de descuento para un plazo de una duración predeterminada, comprendiendo dicha etapa de verificación la verificación de que dicho plazo no ha expirado.
7. Procedimiento de acuerdo con la reivindicación 6, según el cual dicha función de descuento está basada en un reloj material de dicho dispositivo de microcircuitos.
- 60 8. Procedimiento de acuerdo con una cualquiera de las reivindicaciones 5 a 7, comprendiendo el procedimiento además las etapas siguientes:
 - recepción de al menos una información de dicho terminal móvil al que está conectado dicho dispositivo de
65 microcircuitos para informar que al menos un puesto de conexión de acceso sin contacto está accesible a través de dichos medios de comunicación inalámbricos de alcance reducido;

- selección (300) de al menos dicha aplicación protegida integrada en dicho dispositivo de microcircuitos en respuesta a dicha al menos una información recibida, y transmisión de al menos una referencia a dicha al menos una aplicación seleccionada a dicho terminal móvil; y
- 5 - recepción de al menos un identificador de una aplicación, correspondiendo dicho identificador a una referencia a dicha aplicación protegida integrada.
- 9. Procedimiento de acuerdo con una cualquiera de las reivindicaciones precedentes, según el cual dicho dispositivo
- 10 de microcircuitos es una tarjeta de microcircuitos.
- 10. Programa de ordenador que comprende unas instrucciones adaptadas para la realización de cada una de las etapas del procedimiento de acuerdo con una cualquiera de las reivindicaciones precedentes cuando dicho programa se ejecuta en un ordenador.
- 15 11. Dispositivo que comprende unos medios adaptados para la realización de cada una de las etapas del procedimiento de acuerdo con una cualquiera de las reivindicaciones 1 a 9.
- 12. Dispositivo de microcircuitos para controlar la ejecución de al menos una función interna protegida integrada en dicho dispositivo de microcircuitos (150), estando adaptado dicho dispositivo de microcircuitos para ser utilizado en cooperación con un terminal móvil (100), estando este dispositivo caracterizado porque comprende un microcontrolador configurado para realizar las etapas siguientes:
- 20 - detección (400) de una orden de puesta en suspensión de dicho dispositivo de microcircuitos, siendo detectada dicha orden de puesta en suspensión a partir de una información recibida desde un terminal móvil en el que está conectado dicho dispositivo de microcircuitos;
- 25 - análisis (415) de al menos una indicación relativa a la ejecución de dicha al menos una función interna protegida; y
- 30 - si dicha al menos una función interna protegida es susceptible de ser afectada por la ejecución de dicha orden de puesta en suspensión, ejecución (410) diferida de dicha orden de puesta en suspensión.
- 13. Dispositivo según la reivindicación 12, que comprende además al menos una memoria configurada para memorizar al menos un dato relativo a dicha al menos una función interna protegida.
- 35 14. Dispositivo de acuerdo con la reivindicación 13, según el cual dicho microcontrolador está configurado además para ejecutar un algoritmo de criptografía que protege dicho al menos un dato relativo a dicha al menos una función interna protegida.
- 40 15. Dispositivo de acuerdo con una cualquiera de las reivindicaciones 12, 13 y 14, según el cual dicho microcontrolador está configurado además para ejecutar un algoritmo de protección material de al menos un componente de dicho dispositivo.
- 45 16. Tarjeta de identificación de un abonado en una red de telefonía móvil que comprende el dispositivo según una cualquiera de las reivindicaciones 11 a 15.
- 17. Terminal móvil que integra el dispositivo según una cualquiera de las reivindicaciones 11 a 15.

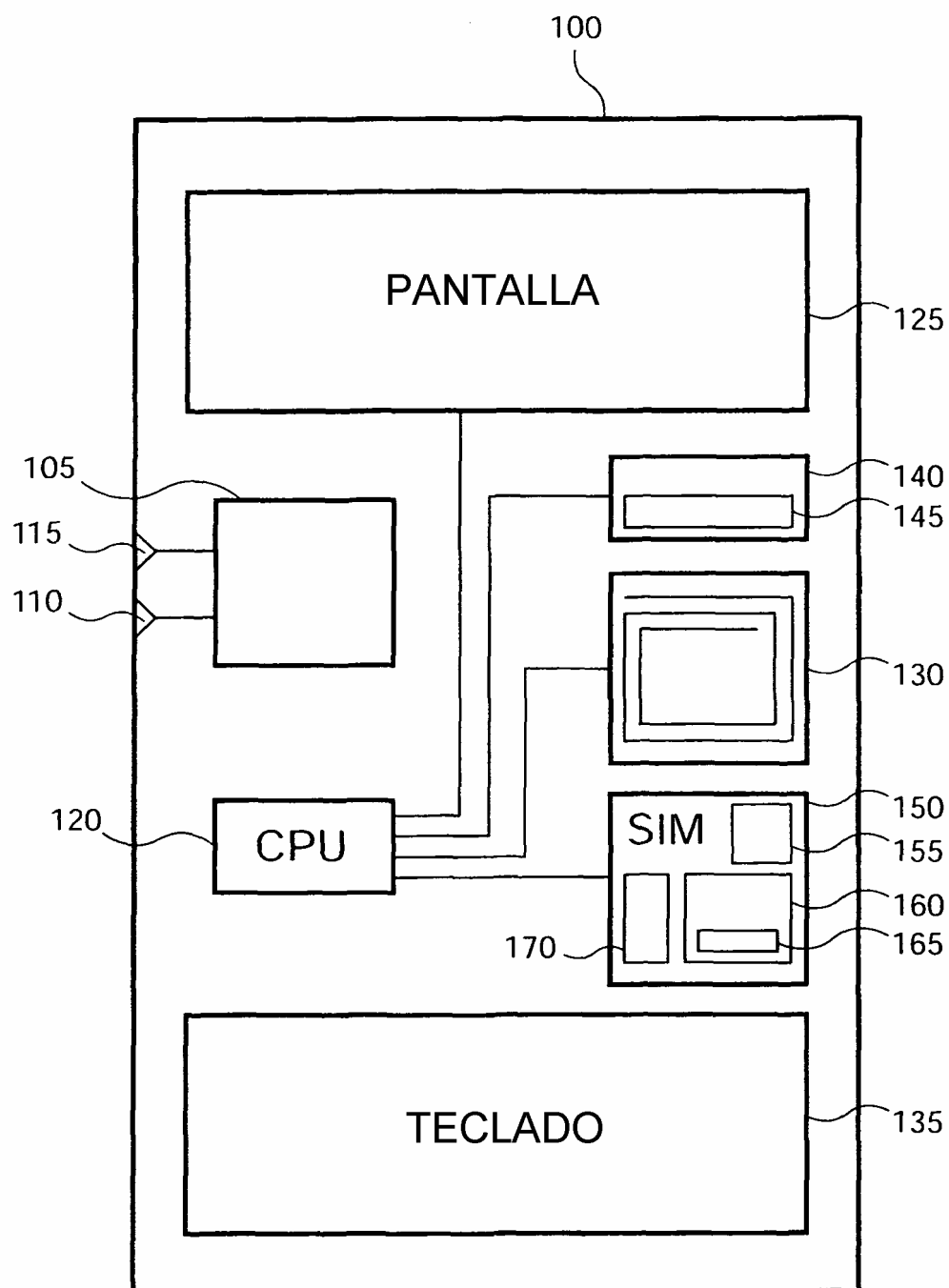


Fig. 1

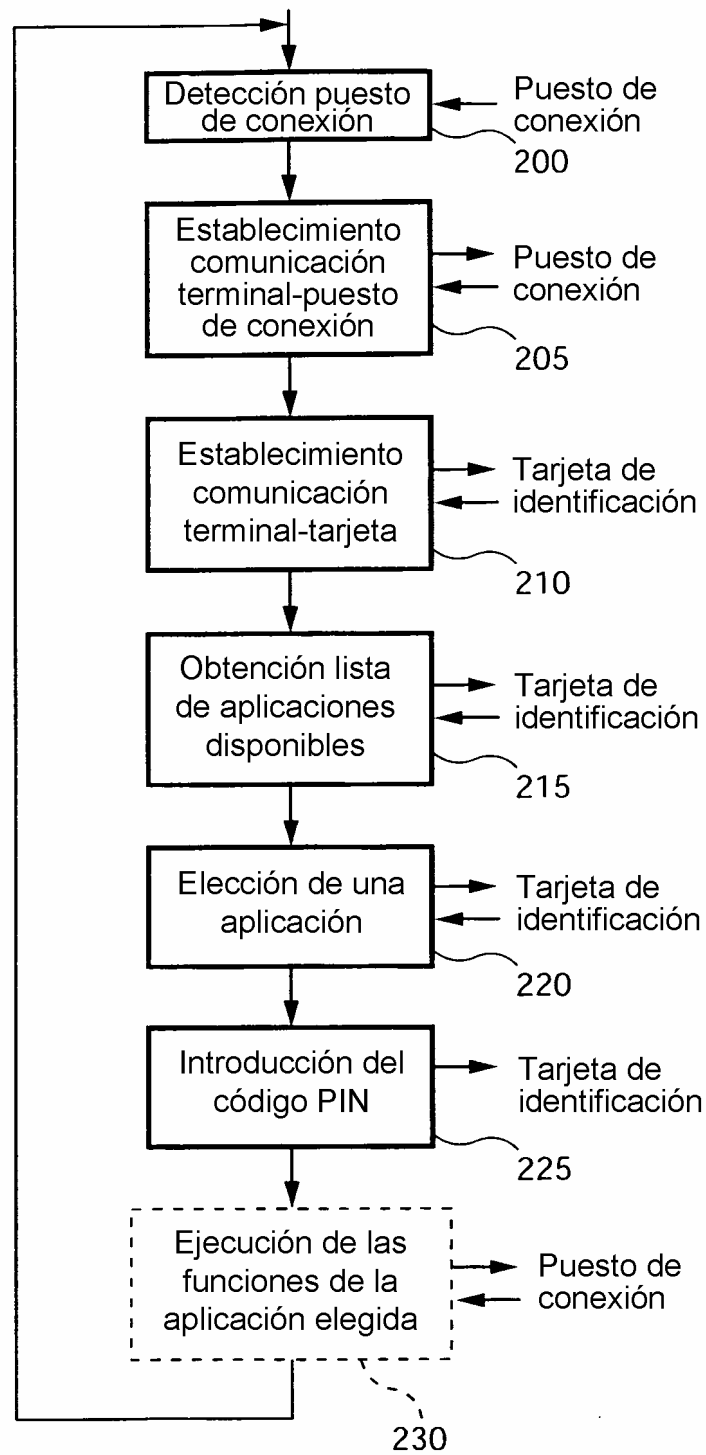


Fig. 2

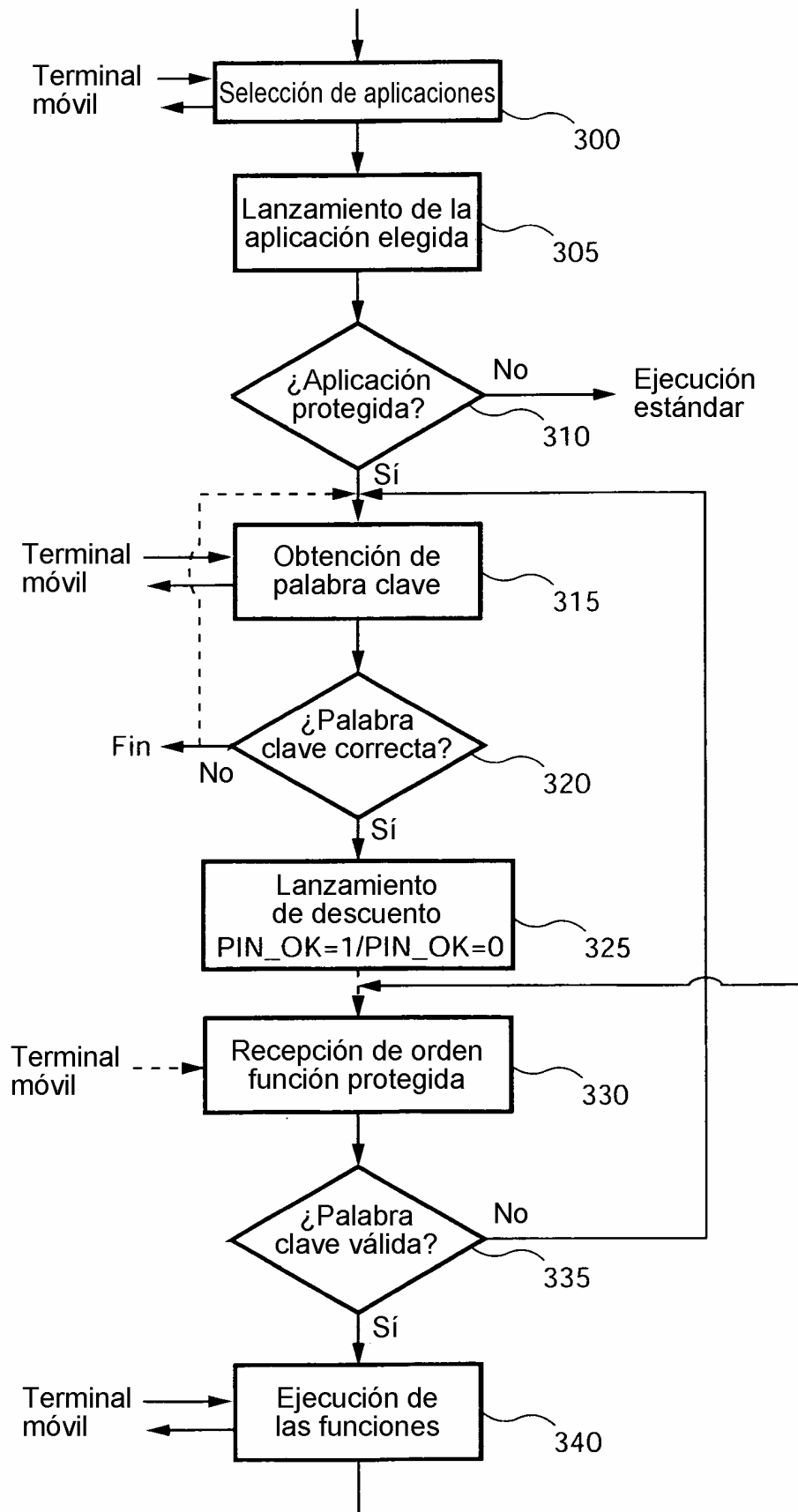


Fig. 3

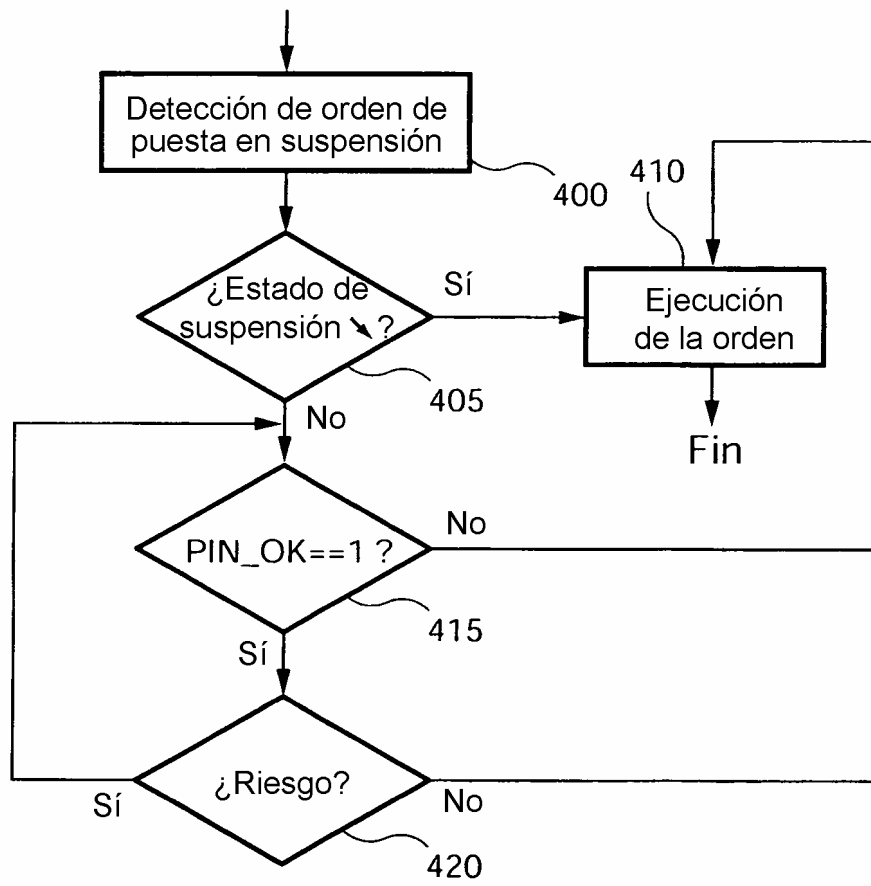


Fig. 4