(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 675 859**

(51) Int. CI.:

G06F 21/00 (2013.01)
G06K 19/07 (2006.01)
G07F 7/10 (2006.01)
H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **10.06.2010 E 10165572 (8)**

(97) Fecha y número de publicación de la concesión europea: **04.04.2018 EP 2264632**

(54) Título: **Dispositivo electrónico con dos interfaces de comunicación y método asociado para asegurar tal dispositivo**

(30) Prioridad:

12.06.2009 US 483498

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
13.07.2018

(73) Titular/es:

OBERTHUR TECHNOLOGIES OF AMERICA CORP. (100.0%)
4250 Pleasant Valley Road
Chantilly VA 20151-1221, US

(72) Inventor/es:

GOYET, CHRISTOPHE

(74) Agente/Representante:

ISERN JARA, Jorge

DESCRIPCIÓN

Dispositivo electrónico con dos interfaces de comunicación y método asociado para asegurar tal dispositivo

La presente invención se refiere un dispositivo electrónico y un método asociado. Se aplica en particular a entidades electrónicas que tienen dos interfaces y medios para procesar un artículo secreto de datos, por ejemplo medios para autenticación del usuario.

Una entidad electrónica, tal como una tarjeta inteligente, por ejemplo, que generalmente incluye circuitos electrónicos capaces de almacenar información, incluye medios para comunicación con el exterior, en particular para intercambiar información mantenida por la entidad electrónica con dispositivos externos, de tipo lector o terminal.

De los medios de comunicación usados ampliamente, se hace una distinción entre medios de comunicación por contacto, para los que un contacto eléctricamente conductor físico entre la entidad electrónica y el terminal es una condición necesaria para el establecimiento de comunicación, y medios de comunicación remota (sin contacto), gracias a los cuales la comunicación entre la entidad electrónica y un lector es posible sin contacto físico entre estos dos elementos, por medio de comunicación por medio de una onda electromagnética, generalmente con un alcance del orden de unos pocos centímetros.

Se conoce el uso de contadores de errores (o fallos) en un microcircuito seguro. Estos contadores de errores se usan, por ejemplo, en tarjetas inteligentes para supervisar el uso de un número de identificación personal (PIN).

Por ejemplo, si la tarjeta recibe un PIN incorrecto, un contador de fallos se incrementa en uno. Si el siguiente PIN es correcto, el contador de fallos se reinicia a cero. Si no, el contador se incrementa de nuevo. De esta manera, el contador de fallos retiene un recuento del número de PIN sucesivos incorrectos. Cuando el valor de este contador alcanza un cierto límite, el uso de la tarjeta se bloquea.

Las tarjetas generalmente están provistas de un mecanismo que autoriza acceso, por medio de diferentes códigos secretos, para desbloquear una tarjeta bloqueada. Normalmente el proveedor de la tarjeta mantiene estos códigos, por ejemplo un banco. Por lo tanto el titular de la tarjeta puede (y debe) dirigirse al proveedor de la tarjeta o una autoridad similar para bloquear su tarjeta.

También se conoce a partir del documento WO 2007/012738 una entidad electrónica que tiene medios de comunicación por contacto y medios de comunicación remota, junto con medios para autorizar un intercambio a través de los medios de comunicación remota como una función de la recepción previa de una instrucción a través de los medios de comunicación por contacto, donde sea apropiado con verificación de que un artículo de activación de información es igual a un valor predeterminado.

Un inconveniente de estos procedimientos es evidente en el caso de tarjetas que tienen una interfaz sin contacto, o más generalmente una interfaz que es fácilmente accesible o más fácilmente accesible que una segunda interfaz por contacto. Un atacante podría usar la interfaz fácilmente accesible para enviar una serie de peticiones de autenticación con códigos de autenticación incorrectos, que tendrían la consecuencia de bloquear la tarjeta sin que se notifique de ello al titular de la tarjeta (ataque de denegación de servicio (DoS)).

Un ataque de este tipo efectuado a gran escala puede provocar un daño considerable a titulares de tarjetas y a proveedores obligados a intervenir para desbloquear las tarjetas bloqueadas de esta manera.

Por lo tanto la invención tiene como objetivo evitar o impedir un ataque de este tipo que tiene como objetivo convertir la entidad electrónica móvil incapaz de responder a las peticiones de su usuario.

En este contexto, se conoce a partir del documento WO 2008/096078 un dispositivo electrónico móvil que incluye dos interfaces y medios de seguridad adaptados para detectar un tipo de ataque y evitar la comunicación usando una de las dos interfaces, teniendo cada interfaz su propio contador de fallos.

Para resolver los problemas a los que se ha hecho referencia, se propone un dispositivo electrónico de acuerdo con la reivindicación 1.

Se asegura el uso del valor secreto, ya que las dos diferentes interfaces se protegen mediante inhibiciones, y además, gracias a la presencia de un valor de indicador por el cual una de las interfaces se inhibe de forma diferente que la otra, el usuario retiene el acceso al valor secreto incluso en el caso de protección mejorada provocada por un ataque del tipo de denegación de servicio.

De acuerdo con una característica ventajosa, los medios para usar un valor secreto incluyen medios de seguridad adaptados para autorizar acceso a una función del dispositivo electrónico móvil en reacción a una autenticación satisfactoria.

Por lo tanto el dispositivo se asocia con un usuario particular u otro dispositivo particular (una máquina), que debe autenticarse antes de que pueda usarse una función de protección del dispositivo.

De acuerdo con una característica, los medios de control se adaptan adicionalmente para actualizar un indicador de uso incorrecto de dichos medios para usar una clave secreta a través de cualquier interfaz.

Por lo tanto para definir el indicador únicamente pueden usarse características de uso incorrecto, evaluadas sobre la base de reglas de uso predefinidas, posiblemente incluyendo un recuento del número de ocurrencias de uso incorrecto.

De acuerdo con una característica ventajosa, el indicador es un recuento de usos incorrectos de los medios de seguridad a través de cualquier interfaz.

De acuerdo con una característica ventajosa, para al menos un valor del indicador, se bloquea la comunicación usando la segunda interfaz, pero se autoriza la comunicación usando la primera interfaz.

Gracias a la presencia de un valor de indicador para el que se bloquea la primera de las interfaces pero no la otra, el usuario retiene el acceso a la función del dispositivo electrónico incluso en el caso de desconexión de una interfaz después de un ataque de denegación de servicio.

De acuerdo con una característica ventajosa, los medios de control se adaptan

- para aplicar dicha primera inhibición si dicho indicador excede de un primer umbral, y
- para aplicar dicha segunda inhibición si dicho indicador excede de un segundo umbral mayor que el primer umbral.

La presencia de dos umbrales diferentes habilita la definición de un intervalo de longitud finita de valores del indicador en el que se aplica una inhibición pero no la otra, protegiendo por lo tanto el dispositivo electrónico móvil sin bloquear el acceso por el usuario a la función o el valor secreto.

De acuerdo con una característica ventajosa, al menos una de las dos inhibiciones incluye la aplicación de un retardo de tiempo después del uso incorrecto de los medios para usar un valor secreto, siendo la comunicación con dichos medios para usar un valor secreto a través de la correspondiente interfaz retardada durante dicho retardo de tiempo y aumentando el retardo de tiempo a una tasa ascendente con el recuento.

El uso de una inhibición en forma de un retardo protege el dispositivo electrónico móvil sin bloquear el acceso por el usuario a la función o al valor secreto, ya que el usuario puede esperar al final del retardo y a continuación usar la interfaz.

Como alternativa, una de las inhibiciones puede incluir la reducción del alcance de comunicación a través de una interfaz sin contacto, por ejemplo a través de cifrado o ralentizando la tasa de bits a través de la interfaz.

De acuerdo con otra característica ventajosa, cada una de las dos inhibiciones incluye aplicación de un retardo de tiempo después de uso incorrecto de los medios para usar un valor secreto, siendo la comunicación con dichos medios para usar un valor secreto a través de la correspondiente interfaz retardada durante dicho retardo de tiempo, aumentando el retardo de tiempo a una tasa ascendente con el recuento, y siendo el retardo de tiempo aplicado en la segunda interfaz al menos el doble del retardo de tiempo aplicado en la primera interfaz para el mismo recuento.

Esta característica asegura ambas interfaces, mientras que habilita que un usuario recupere el uso de cada una de las dos interfaces esperando lo suficiente y haciendo una de las interfaces más disponible al usuario que la otra.

En algunas realizaciones, la segunda interfaz es más accesible a un ataque, por ejemplo del tipo de denegación de servicio, que la primera interfaz.

Por lo tanto la invención protege el dispositivo primeramente contra ataques que se dirigen a la interfaz más accesible, ya que para al menos un valor de recuento se autoriza la comunicación a través de la segunda interfaz menos accesible.

En una realización beneficiosa, los medios de control se adaptan para contar fallos sucesivos de autenticación, estando el dispositivo adaptado para inicializar el indicador en reacción a la detección de una autenticación satisfactoria.

Esta característica muestra, cuando la autenticación ha sido satisfactoria, que un usuario autorizado ha usado el dispositivo, y que no es necesario bloquear el dispositivo inmediatamente si los medios de seguridad se usan incorrectamente posteriormente en el siguiente uso.

En una realización, los medios de recuento se adaptan para contar fallos de autenticación dentro de un periodo de tiempo continuo de longitud predefinida.

Los medios para usar un valor secreto ventajosamente usan un código secreto de identificación personal.

Como alternativa, los medios de seguridad usan una clave criptográfica o datos biométricos. Estos diferentes medios de seguridad pueden combinarse.

Dicha segunda interfaz ventajosamente incluye medios de recepción de datos que usan un protocolo de comunicación sin contacto, por ejemplo uno de conformidad con la norma ISO 14443.

De acuerdo con una característica ventajosa, dicha primera interfaz incluye medios para recibir datos que usan un protocolo de comunicación por contacto, por ejemplo usando un protocolo de conformidad con la norma ISO 7816.

En diferentes realizaciones, el dispositivo es una tarjeta inteligente o una llave USB.

El dispositivo puede además cumplir con la FIPS o con la norma de criterio común.

La invención también propone un método de acuerdo con la reivindicación 11. Gracias al uso de este método, se asegura el uso del valor secreto, ya que las dos diferentes interfaces se protegen mediante inhibiciones, y además, gracias a la presencia de un valor de recuento por el cual una de las interfaces se inhibe de forma diferente que la otra, el usuario retiene el acceso al valor secreto incluso en el caso de protección mejorada provocada por un ataque del tipo de denegación de servicio.

En algunas aplicaciones del método de la invención, como una función de los usos hechos del dispositivo, el método también incluye etapas de petición de un código de identificación del usuario y de verificación de que un código de identificación proporcionado por el usuario a través de la interfaz sin contacto es correcto.

En el caso de un resultado positivo, se abre acceso a una función y en el caso de un resultado negativo, en el contexto de recuento, se incrementa un contador de intentos fallidos.

En algunas realizaciones del método, únicamente se cuentan usos incorrectos.

La Figura 1 muestra una entidad electrónica de una realización de la invención.
La Figura 2 representa un terminal electrónico capaz de comunicar con una entidad electrónica de la invención.
La Figura 3 representa en forma de diagrama un componente electrónico incluido en una entidad electrónica de la invención.
La Figura 4 representa etapas de una realización de un método de la invención.
La Figura 5 representa etapas ejecutadas en el caso de ciertos usos de una entidad electrónica de la invención.

Haciendo referencia a la Figura 1, la tarjeta de microcircuito 1000 incluye adicionalmente un microcontrolador 1100, contactos enrasados 1200 en la superficie de la tarjeta 100 de conformidad con la norma ISO 7816 y una antena 1300. El microcontrolador también es capaz de intercambiar información de entrada y salida a través de o bien los contactos enrasados 1200 o bien a través de la antena 1300.

El microcontrolador 1100 se alimenta eléctricamente mediante un campo magnético alterno a través de la antena 1300 o a través de los contactos enrasados 1200. También puede alimentarse mediante una fuente de energía interna.

Teniendo dos interfaces de comunicación, la tarjeta 1000 se denomina como tarjeta dual.

Se adapta en particular para usar, a través de la antena 1300, un protocolo de comunicación sin contacto diseñado para la comunicación a distancia de hasta 20 centímetros, por ejemplo de acuerdo con la norma ISO 14443 o la norma NFC (Comunicación de Campo Cercano) o el protocolo ZigBee™ para la comunicación a distancias mayores, de unos pocos metros.

Haciendo referencia a la Figura 2, el terminal 2000 es un terminal de pago sin contacto que incluye una pantalla 2400, un teclado 2500 y una interfaz de radio sin contacto 2300.

El microcontrolador 1110 de la tarjeta 1000 y el terminal 2000 se adaptan para comunicar a través de la antena 1300 y la interfaz de radio 2300 usando un protocolo de comunicación de conformidad con las normas apropiadas, por ejemplo las referidas anteriormente.

El microcontrolador 1100 contiene en su memoria no volátil instrucciones relacionadas con una aplicación 1110, que puede ser un sistema operativo o cualquier otra aplicación, incluyendo el mismo diferentes módulos de aplicación vinculados o independientes. La memoria no volátil puede ser una memoria de sólo lectura (ROM), por ejemplo.

La aplicación 1110 incluye un módulo o código 1112 para verificar un número de identificación personal (PIN). El microcontrolador incluye un registro 1114 que almacena el PIN asociado con la tarjeta de microcircuito 1000. Este registro puede almacenarse en una memoria no volátil regrabable, por ejemplo una EEPROM (Memoria de Sólo Lectura Eléctricamente Borrable y Programable) o una memoria flash o donde sea apropiado en una memoria de sólo lectura.

La aplicación 1110 incluye una función 1111 cuya ejecución por el microcontrolador 1100 se condiciona por la comunicación exitosa del número de identificación personal (PIN) al microcontrolador 1100 a través de una de las interfaces de comunicación.

Esta función 1111 puede ser la ejecución de una aplicación de software (autónoma o incluida en una aplicación más extensa) almacenada en el microcontrolador 1100 o acceso a una memoria del microcontrolador 1100. Puede ser una aplicación de pago, por ejemplo para efectuar una transacción de conformidad con la norma Europay Mastercard Visa (EMV).

El microcontrolador 1100 también incluye un registro 1113 (o registro de memoria) que almacena un número de comunicaciones incorrectas sucesivas de un PIN, a medida que se detectan por el código de verificación de PIN 1112. Este registro 1113 puede almacenarse en una memoria no volátil regrabable, por ejemplo una EEPROM o una memoria flash.

Todas las instancias de comunicación erróneas se cuentan de esta manera, ya sea usando la antena 1300 o los contactos enrasados 1200.

En una realización ilustrativa, el contenido del registro 1113 se inicializa al número de fallos máximo aceptable (que puede establecerse en el valor 3, por ejemplo), más allá del cual la tarjeta se bloquea.

Haciendo referencia a la Figura 4, el titular de la tarjeta 1000 usa la tarjeta en un terminal 2000 para llevar a cabo una transacción sin contacto a través de la antena 1300 y la interfaz de radio 2300. Este proceso comienza con una etapa 4005 de iniciación de comunicación de campo cercano entre la tarjeta y el terminal.

Durante una etapa 4010, el terminal de pago sin contacto 2000 muestra en su pantalla 2400 un mensaje solicitando al usuario que introduzca su PIN. El usuario introduce en el terminal un valor PIN P usando el teclado 2500.

Durante una etapa 4020, el valor P se envía al sistema operativo 1110 a través de la interfaz de radio 2300 y la antena 1300 en una orden de APDU (unidad de datos de protocolo de aplicación) entre una tarjeta de microcircuito y un lector asociado, como se define por la norma ISO 7816. En la realización mostrada, esta es la orden VERIFICAR PIN (ISO 7816).

En esta fase de la ejecución del método, la aplicación 1110 está en una posición para tener en cuenta la información al efecto que el valor P se envió a la misma a través de la interfaz sin contacto 1300. Esto es posible si el programa que se ejecuta (Figura 4) es específico a la situación en la que el valor P se envió a través de la interfaz sin contacto y está por lo tanto separado del programa que se está ejecutando cuando el valor P se envió a través de la interfaz por contacto (véase la Figura 5, como se describe a continuación). La aplicación 1110 por lo tanto contiene dos subaplicaciones 1110a y 1110b.

Como alternativa, la aplicación 1110 puede almacenar información al efecto de que el valor P se envió a través de la interfaz sin contacto. Esta información, que puede ser booleana o binaria, puede almacenarse en una memoria de acceso aleatorio (RAM) u otra memoria volátil del microcontrolador 1100. Puede actualizarse después de la etapa 4005 o después de la etapa 4020 y el programa a continuación incluye, cuando sea necesario, etapas de prueba para verificar el valor de esta información.

Durante una etapa 4030, la aplicación 1110 verifica si el contenido del registro 1113 es estrictamente mayor de 1.

De acuerdo con una variante, la aplicación 1110 verifica si el contenido del registro 1113 es estrictamente mayor de 2 u otro valor predefinido si el contador se inicializa a un valor mayor de 2.

Si es así, la aplicación 1110 inicia la aplicación de verificación 1112 que compara el contenido del registro 1114 con P durante una etapa 4040.

Si el contenido del registro 1114 es igual al valor P, entonces la aplicación 1110 inicia la función 1111, durante una etapa 4050, y el contenido del registro 1113 se reinicializa al número de intentos autorizados, durante una etapa 4060. El número de intentos autorizados es un valor almacenado en una memoria (memoria de sólo lectura o memoria volátil) del microcontrolador 1100 y que no se modifica durante la ejecución del método al que se refiere la invención.

Para efectuar esta reinicialización, la tarjeta 1000 por lo tanto incluye medios (no mostrados) para inicializar el contenido del registro 1113, esos medios pueden incluirse en la aplicación 1110.

Si el contenido del registro 1114 es diferente de P, entonces la aplicación 1110 disminuye el contenido del registro 1113 durante una etapa 4070, después de la cual comienza una nueva iteración del algoritmo que se acaba de describir, comenzando con la etapa de interrogación a través de la pantalla 4010.

Si el contenido del registro 1113 no es estrictamente mayor de 1, entonces la aplicación 1100 efectúa una etapa de prueba 4080 para averiguar si el contenido del registro 1113 es igual a 0.

Si el contenido del registro 1113 es diferente de 0 (es decir en condiciones normales de uso si es igual a 1), la aplicación 1110 envía, durante una etapa 4090, al terminal 2000 a través de la antena 1300 y la interfaz de radio 2300 una respuesta de APDU de "CONDICIÓN DE USO NO SATISFECHA" de conformidad con la norma ISO 7816, indicando al terminal que no se cumplen las condiciones para acceso mediante la orden de APDU usada anteriormente ("Verificar PIN" a través de la interfaz sin contacto).

El resultado para el usuario es la necesidad de usar la interfaz por contacto. El terminal a continuación muestra un mensaje que indica al usuario que la interfaz sin contacto se ha desactivado, durante una etapa 4100.

En una realización, la aplicación 1110 almacena en una memoria del microcontrolador información que indica que la interfaz sin contacto está bloqueada o que el acceso a la función 1111 a través de la interfaz sin contacto está prohibido. Este artículo de información preferentemente booleana se almacena en una memoria no volátil regrabable del microcontrolador 1100. En otra realización, el contenido del registro 1113 sirve como una información equivalente, siendo el hecho de que es menor o igual a 1 suficiente para indicar que la interfaz sin contacto está bloqueada.

A la inversa, si el contenido del registro 1113 es igual a 0, entonces la aplicación 1110, durante una etapa 4110, envía al terminal 2000 a través de la antena 1300 y la interfaz de radio 2300 una respuesta de APDU de "MÉTODO DE AUTENTICACIÓN BLOQUEADO" de conformidad con la norma ISO 7816 (esto significa que el uso de la tarjeta se bloquea por los medios de seguridad, es decir el código 1112, y se bloquea ese uso de la función 1111).

El terminal 2000 a continuación muestra un mensaje en su pantalla indicando al usuario que la tarjeta 1000 está bloqueada, durante una etapa 4120.

En una realización, la aplicación 1110 almacena en una memoria del microcontrolador 1100 información que indica que la tarjeta 1000 está bloqueada o que el acceso a la función 1111 está prohibido, cualquiera que sea la interfaz que se usa. Esta información preferentemente booleana se almacena en una memoria no volátil regrabable del microcontrolador 1100. En otra realización, el contenido del registro 1113 sirve como una información equivalente, siendo el hecho de que es menor o igual a 0 suficiente para indicar que la tarjeta está bloqueada o que el acceso a la función 1111 está prohibido, cualquiera que sea la interfaz que se usa.

Haciendo referencia a la Figura 5, el titular de la tarjeta 1000 usa la tarjeta en un terminal 3000 capaz de comunicar con la tarjeta 1000 por contacto de acuerdo con una norma compatible con los contactos enrasados 1200. El terminal 3000 puede ser el mismo terminal 2000 descrito anteriormente, para un dispositivo diferente.

El proceso de comunicación comienza con una etapa 5005 de desencadenamiento de comunicación de la tarjeta y el terminal por contacto.

Durante una etapa 5010, el terminal muestra en su pantalla un mensaje que avisa al usuario que introduzca su PIN. El usuario introduce en el terminal un valor PIN P usando el teclado, y ese valor se envía al microcontrolador 1100 durante una etapa 5020, a través de los contactos enrasados 1200.

En esta fase de la ejecución del método, la aplicación 1110 está en una posición para tener en cuenta del hecho de que el valor P se envió a la misma a través de la interfaz por contacto 1200. Como se ha explicado anteriormente con referencia a la Figura 4, esto es posible si el programa que se está ejecutando (Figura 5) es específico al caso en el que el valor P se envió a través de la interfaz sin contacto, y está por lo tanto separado del programa que se está ejecutando cuando el valor P se envió a través de la interfaz por contacto (Figura 4).

Como alternativa, la aplicación 1110 puede almacenar información al efecto de que el valor P se envió a la misma a través de la interfaz por contacto 1200. Como anteriormente, esta información puede almacenarse en una memoria volátil regrabable, por ejemplo una RAM del microcontrolador 1100. Puede actualizarse después de la etapa 5005 o después de la etapa 5020, dependiendo de la realización.

Durante una etapa 5030, la aplicación 1110 verifica si el contenido del registro 1113 es mayor que el valor 0.

Si es así, la aplicación 1110 inicia el código de verificación 1112 que compara el contenido del registro 1114 con el valor P, durante una etapa 5040.

Si el resultado de esta última comparación es positivo, es decir si el contenido del registro 1114 es igual al valor P, entonces la aplicación 1110 inicia la función 1111, durante una etapa 5050, y el contenido del registro 1113 se reinicializa al número máximo de intentos autorizados, que como se ha explicado anteriormente se contiene y conserva sin cambios en una memoria del microcontrolador durante el uso normal de la tarjeta 1000.

Si el contenido del registro 1114 es diferente de P, entonces el sistema operativo 1110 disminuye el contenido del registro 1113 por una unidad, durante una etapa 5070.

Si, durante la etapa 5030, la aplicación 1110 encuentra que el contenido del registro 1113 no es estrictamente mayor de 0, entonces, durante una etapa 5080, la aplicación 1110 envía al terminal 3000 a través de los contactos enrasados 1200 una respuesta de APDU de " MÉTODO DE AUTENTICACIÓN BLOQUEADO".

El terminal 3000 a continuación muestra un mensaje en su pantalla indicando al usuario que la tarjeta 1000 se bloquea, durante una etapa 5090.

Por consiguiente, gracias al método ejecutado en la tarjeta, el último se proyecta contra un ataque del tipo de denegación de servicio en la interfaz sin contacto (la antena 1300), ya que si el último es atacado, la comunicación a través de la antena se bloquea (etapas 4090 y 4100) cuando el contenido del registro 1113 alcanza 1, pero la comunicación a través del contacto enrasado es aún posible.

En una realización alternativa, el titular de la tarjeta inteligente se autentica mediante la orden AUTE EXTERNA (ISO 7816).

En una realización alternativa adicional, el módulo 1112 autentica al usuario por medio de una clave criptográfica (u otros datos secretos) o datos biométricos tal como una huella dactilar.

En otra realización, el registro 1113 no se disminuye durante las etapas 4070 y 5070, sino que se incrementa. En este caso, las etapas de comparación 4030 y 5030, que son del tipo de "¿está el contenido del registro por encima de un valor límite?", se sustituyen por las etapas de comparación del tipo "¿está el contenido del registro por debajo de un valor límite?".

En otra realización, el registro 1113 contiene, en lugar de un valor vinculado al número de fallos sucesivos, un número de usos de la tarjeta desde una cierta fecha, o en un periodo pasado predefinido relativo al tiempo en el que se actualiza el contenido del registro. Los usos contados de esta manera pueden ser intentos de autenticación (que conducen a éxito o fallo), u otra forma de uso de la tarjeta 1000, de una de sus funciones, o un intento a tal uso, en el entendimiento de que el uso por encima de una frecuencia dada en esta realización constituye un uso incorrecto de la tarjeta.

Una forma de uso que es de interés en particular en el contexto de esta variante es el uso de un valor secreto, por ejemplo una clave criptográfica almacenada en la memoria del microcontrolador 1100, por ejemplo en el registro 1114, siendo este uso desencadenando por la recepción de una orden (por ejemplo una orden de APDU, de conformidad con la norma ISO 7816) a través de la interfaz 1200 o 1300. El código 1112 efectúa cifrado o descifrado usando la clave y el registro 1113 se usa para almacenar un valor vinculado a un recuento de operaciones de cifrado o descifrado usando la clave, o de usos de los datos secretos.

Por lo tanto el contenido del registro 1113 puede usarse para evaluar la frecuencia de uso durante un periodo de tiempo definido. La frecuencia de uso determinada de esta manera se compara con una frecuencia de límite predeterminada de valor de uso (por ejemplo 1000 usos en un periodo de tiempo definido). En este contexto, un gran número de usos o una alta frecuencia de uso puede considerarse como característica de un ataque del tipo de análisis de potencia diferencial, medido además mediante el análisis del consumo de potencia de la tarjeta.

En otra realización, el registro 1113 contiene en lugar de un valor vinculado al número de usos un valor vinculado al número de fallos de autenticación desde una cierta fecha o en un periodo pasado predefinido relativo al tiempo en el que el registro se actualiza.

Por lo tanto el contenido del registro puede usarse para evaluar la frecuencia de fallos de autenticación durante un periodo de tiempo definido. La frecuencia determinada de esta manera se compara con un valor límite de frecuencia de fallos de autenticación predeterminado. Si se alcanza un primer valor límite, únicamente se autoriza el uso de la interfaz por contacto. Si se alcanza un segundo valor límite, mayor que el primer límite, se bloquea el uso de ambas interfaces.

En realizaciones alternativas adicionales, después de un intento fallido de autenticación a través de la interfaz sin contacto 1300, la aplicación 1110 no envía una respuesta de bloqueo al terminal 2000 (en la etapa 4090), sino que

efectúa una etapa de retardo de tiempo de duración T y modifica el contenido de un registro de contador (de una manera similar a la etapa 4070), antes de proceder a otra iteración que comienza con la interrogación a través de la pantalla (similar a la etapa 4010) y que implica un intento (satisfactorio o fallido, como una función de circunstancias) de autenticación, implicando el uso del módulo de verificación 1112.

En realizaciones ventajosas, la duración T aumenta con el número de fallos de autenticación en un periodo de referencia, determinado por el contenido de un registro, disminuido (o incrementado, dependiendo de la implementación) en cada fallo de autenticación. Una vez más el periodo de referencia puede ser el periodo que pasa desde la última autenticación satisfactoria.

La forma de crecimiento puede ser una multiplicación del valor de T por un factor de multiplicación n en cada fallo, siendo n igual a 2 por ejemplo (es decir crecimiento exponencial, también conocido como crecimiento geométrico).

En una realización beneficiosa, después de un intento fallido de autenticación a través de la interfaz sin contacto 1300, la aplicación 1110 se adapta para efectuar una etapa de retardo de tiempo de duración T como se ha explicado anteriormente y, después de otro intento fallido de autenticación, esta vez a través de la interfaz por contacto 1200, también para efectuar una etapa de retardo de tiempo de duración T'.

El tiempo de duración T' se hace entonces diferente de la duración T, por ejemplo el doble de largo, o tres veces de largo. La duración T' también puede evolucionar exponencialmente, con el mismo factor de multiplicación que la duración T, o en una realización con un factor de multiplicación mayor.

En una realización adicional, la aplicación 1110 se adapta para efectuar una etapa de retardo de tiempo de duración T como se ha explicado anteriormente, aumentando la duración T con el número de fallos observados en un periodo de tiempo predefinido. La aplicación 1110 también se adapta, durante una etapa similar a la etapa 4090 anteriormente descrita, para enviar al terminal 2000 a través de la antena 1300 y la interfaz de radio 2300 una respuesta APDU de "CONDICIÓN DE USO NO SATISFECHA", de conformidad con ISO 7816, indicando que la autenticación a través de la interfaz por contacto 1200 ya no es funcional.

En esta realización, la aplicación 1110 primero efectúa etapas de retardo de tiempo y a continuación, si el número de fallos de autenticación excede de un valor límite predeterminado - o umbral - representado por L, la aplicación 1110 procede a desactivar la interfaz 1200, de la manera descrita. El límite L puede tomar un valor de 5, 6 o 10 ocurrencias, por ejemplo.

En esta realización, también es posible que la autenticación a través de la interfaz por contacto 1200 permanezca autorizada cualquiera que sea el número de fallos observados, pero con etapas de retardo de tiempo de duración en aumento entre cada interrogación del usuario a través de la pantalla (etapa 5010) y la siguiente.

Las realizaciones y realizaciones alternativas que se acaban de describir constituyen meramente posibles realizaciones de la invención, que no se limita a las mismas.

En particular, en realizaciones alternativas, la tarjeta inteligente 1000 se sustituye por una llave USB (Bus Serial Universal), un terminal móvil de comunicación, un asistente digital personal o un pasaporte. En algunas realizaciones, este dispositivo está en conformidad con las FIPS (Normas Federales de Procesamiento de la Información) o con la norma de criterio común (CC). En el caso de una llave USB, los contactos enrasados 1200 son los de un conector USB, por ejemplo.

REIVINDICACIONES

1. Dispositivo electrónico móvil (1000), caracterizado por que incluye una primera interfaz (1200) adaptada para establecer comunicación con una entidad electrónica externa
una segunda interfaz (1300) también adaptada para establecer comunicación con una entidad electrónica externa,
medios (1111, 1112, 1114) para procesar un valor secreto, adaptado para reaccionar a la recepción de un mensaje a través de cualquier interfaz
medios de control (1110) adaptados

- para actualizar un indicador (1113) para contar usos incorrectos de dichos medios para usar un valor secreto a través de cualquier interfaz,
- para aplicar una primera inhibición para comunicación usando la primera interfaz como una función de dicho indicador,
- para aplicar una segunda inhibición para comunicación usando la segunda interfaz como una función de dicho indicador,

siendo el dispositivo de tal forma que para al menos un valor del indicador, la segunda inhibición es diferente de la primera,
en el que dicha segunda interfaz (1300) incluye medios de recepción de datos que usan un protocolo de comunicación sin contacto y dicha primera interfaz (1200) incluye medios para recibir datos que usan un protocolo de comunicación por contacto,
en el que se usan dos umbrales diferentes para aplicar respectivamente la primera y la segunda inhibiciones,
en el que para al menos un valor del indicador que corresponde al intervalo de valores del indicador definido por los dos umbrales diferentes, comunicación usando la segunda interfaz y sin contacto (1300) está bloqueada, mientras comunicación usando la primera interfaz y por contacto (1200) está autorizada.

2. Dispositivo de acuerdo con la reivindicación 1, caracterizado por que los medios para usar un valor secreto incluyen medios de seguridad (1112, 1114) adaptados para autorizar acceso a una función (1111) del dispositivo electrónico móvil en reacción a una autenticación satisfactoria.

3. Dispositivo de acuerdo con la reivindicación 1 o la reivindicación 2, caracterizado por que los medios de control (1110) están adaptados adicionalmente para actualizar un indicador de uso incorrecto de dichos medios para usar una clave secreta a través de cualquier interfaz.

4. Dispositivo electrónico móvil (1000) de acuerdo con una cualquiera de las reivindicaciones 1 a 3, caracterizado por que el indicador es un recuento de usos incorrectos de los medios de seguridad (1112, 1114) a través de cualquier interfaz.

5. Dispositivo electrónico móvil de acuerdo con una cualquiera de las reivindicaciones 1 a 4, caracterizado por que al menos una de las dos inhibiciones incluye aplicación de un retardo de tiempo después del uso incorrecto de los medios (1111, 1112, 1114) para procesar un valor secreto, siendo la comunicación con dichos medios para usar un valor secreto a través de la correspondiente interfaz retardada durante dicho retardo de tiempo y aumentando el retardo de tiempo a una tasa ascendente con el recuento.

6. Dispositivo electrónico móvil (1000) de acuerdo con una cualquiera de las reivindicaciones 1 a 5, caracterizado por que cada una de las dos inhibiciones incluye aplicación de un retardo de tiempo después de uso incorrecto de los medios (1111, 1112, 1114) para procesar un valor secreto, siendo la comunicación con dichos medios para usar un valor secreto a través de la correspondiente interfaz retardada durante dicho retardo de tiempo, aumentando el retardo de tiempo a una tasa ascendente con el recuento, y siendo el retardo de tiempo aplicado en la segunda interfaz (1300) al menos el doble del retardo de tiempo aplicado en la primera interfaz (1200) para el mismo recuento.

7. Dispositivo electrónico móvil (1000) de acuerdo con una cualquiera de las reivindicaciones 1 a 6, caracterizado por que la segunda interfaz (1300) es más accesible a un ataque, por ejemplo de tipo de denegación de servicio, que la primera interfaz (1200).

8. Dispositivo de acuerdo con una cualquiera de las reivindicaciones 1 a 7, caracterizado por que los medios de control (1110) están adaptados para contar fallos sucesivos de autenticación, estando el dispositivo adaptado para inicializar el indicador en reacción a la detección de una autenticación satisfactoria.

9. Dispositivo de acuerdo con una cualquiera de las reivindicaciones 1 a 8, caracterizado por que los medios (1111, 1112, 1114) para procesar un valor secreto procesan un código secreto de identificación personal.

10. Dispositivo de acuerdo con una cualquiera de las reivindicaciones 1 a 9, caracterizado por que es una tarjeta inteligente (1000) o una llave USB.

11. Método de uso de un dispositivo electrónico móvil (1000) que tiene primera y segunda interfaces (1200, 1300), en el que la segunda interfaz (1300) incluye medios de recepción de datos que usan un protocolo de comunicación sin contacto y la primera interfaz (1200) incluye medios para recibir datos que usan un protocolo de comunicación por contacto,
caracterizado por que incluye etapas de

- contar usos incorrectos de medios (1111, 1112, 1114) para procesar un valor secreto a través de cualquier interfaz hasta un primer umbral de recuento
- inhibir la comunicación usando la segunda interfaz (1300) bloqueando la segunda interfaz sin contacto (1300), mientras la comunicación usando la primera interfaz por contacto (1200) está autorizada
- contar usos incorrectos hasta un segundo umbral mayor que el primer umbral
- inhibir la comunicación usando la primera interfaz por contacto (1200).

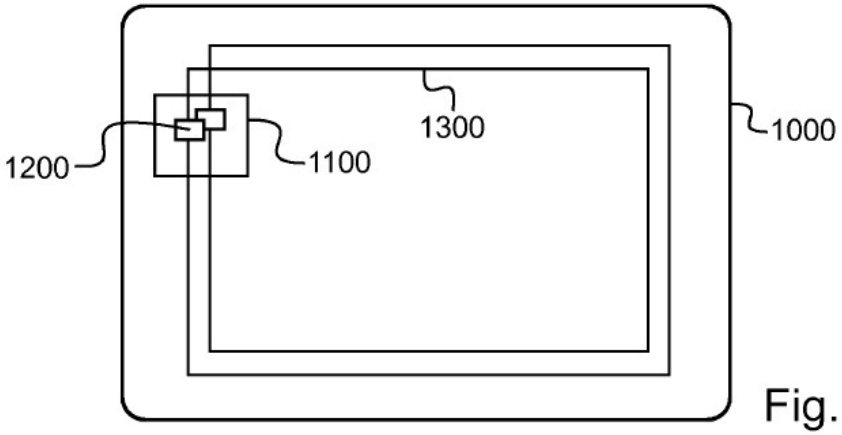

Fig. 1

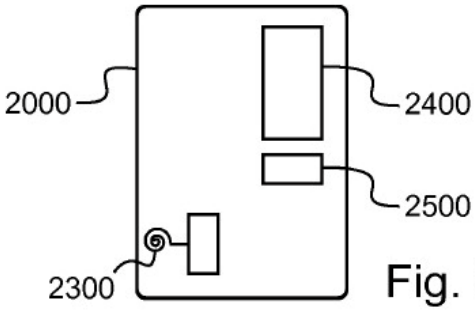

Fig. 2

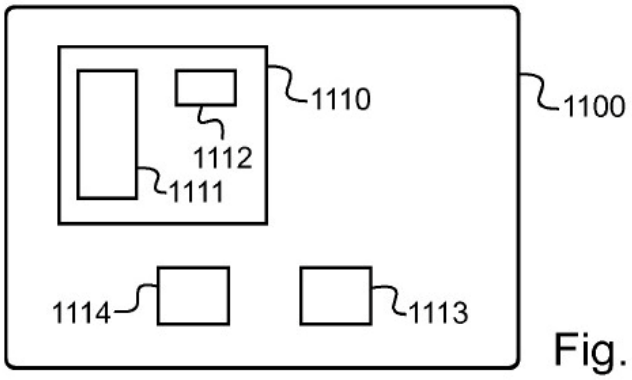

Fig. 3

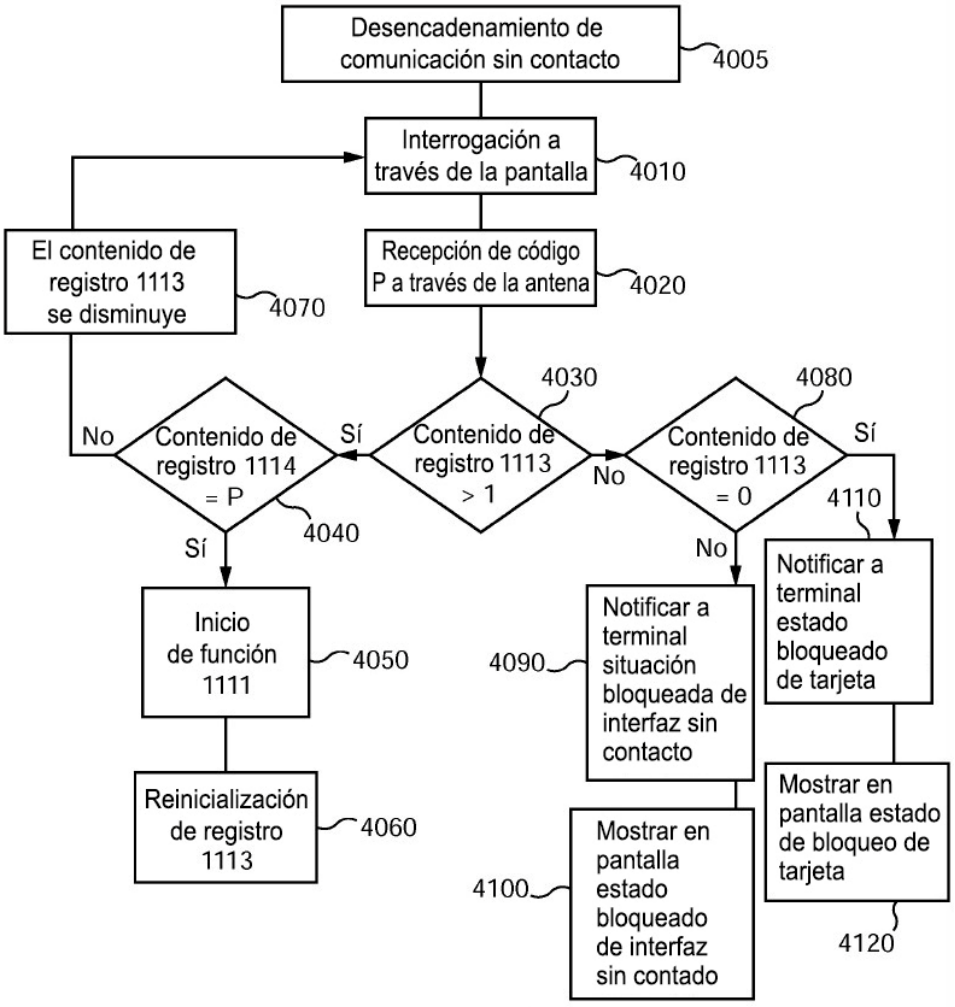
Desencadenamiento de comunicación sin contacto
4005
Interrogación a través de la pantalla
4010
El contenido de registro 1113 se disminuye
4070
Recepción de código P a través de la antena
4020
4030
4080
No
Contenido de registro 1114 = P
Sí
Contenido de registro 1113 > 1
No
Contenido de registro 1113 = 0
Sí
4040
4110
Sí
No
Inicio de función 1111
4050
Notificar a terminal estado bloqueado de tarjeta
4090
Notificar a terminal situación bloqueada de interfaz sin contacto
Reinicialización de registro 1113
4060
Mostrar en pantalla estado de bloqueo de tarjeta
4100
Mostrar en pantalla estado bloqueado de interfaz sin contado
4120

Fig. 4

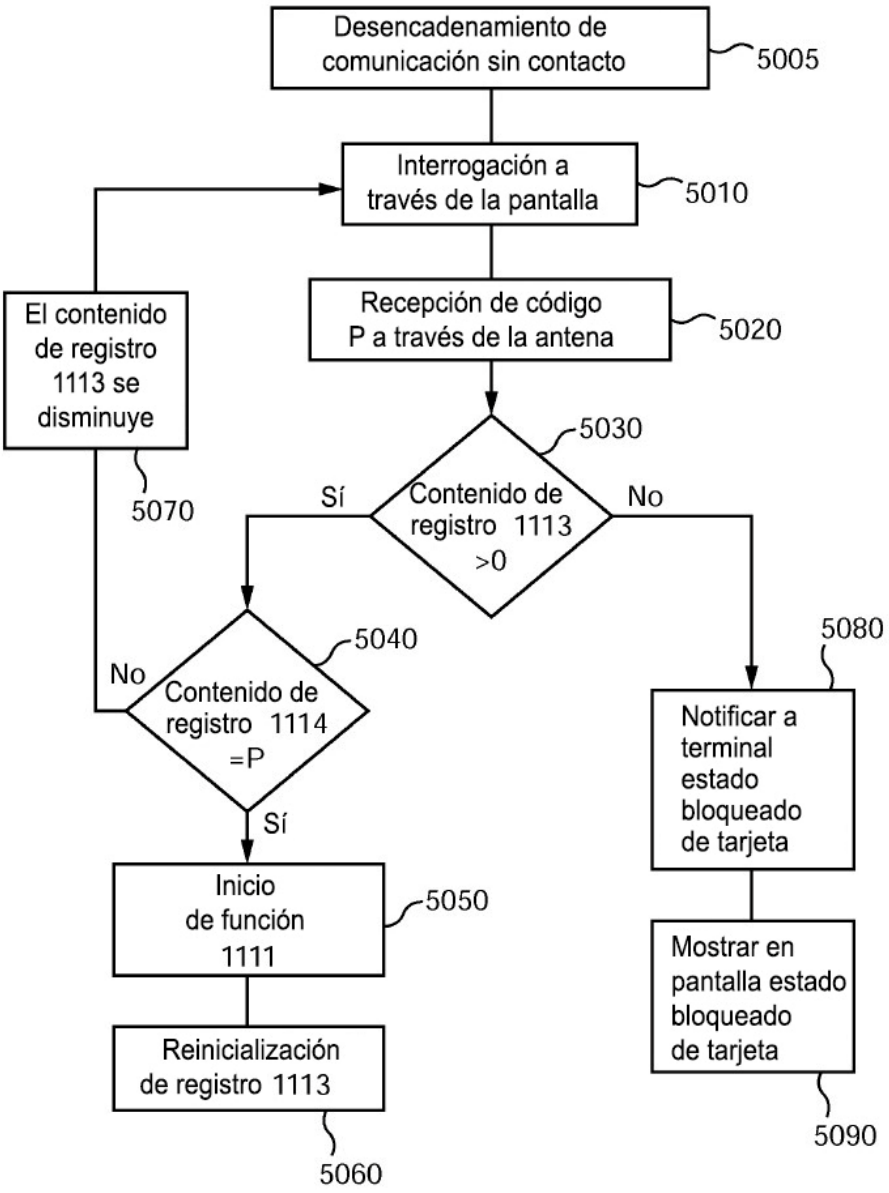
Desencadenamiento de comunicación sin contacto
5005
Interrogación a través de la pantalla
5010
Recepción de código P a través de la antena
5020
5030
Contenido de registro 1113 >0
Sí
No
El contenido de registro 1113 se disminuye
5070
5040
Contenido de registro 1114 =P
No
Sí
Inicio de función 1111
5050
Reinicialización de registro 1113
5060
5080
Notificar a terminal estado bloqueado de tarjeta
Mostrar en pantalla estado bloqueado de tarjeta
5090

Fig. 5