(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 707 504**

(51) Int. CI.:

G06K 7/08 (2006.01)
G06Q 20/40 (2012.01)
G06Q 20/34 (2012.01)
G06Q 20/42 (2012.01)
G07F 7/10 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **10.04.2015 PCT/EP2015/057844**

(87) Fecha y número de publicación internacional: **22.10.2015 WO15158621**

(96) Fecha de presentación y número de la solicitud europea: **10.04.2015 E 15713951 (0)**

(97) Fecha y número de publicación de la concesión europea: **24.10.2018 EP 3132403**

(54) Título: **Dispositivo de procesamiento de datos procedentes de una tarjeta inteligente sin contacto, procedimiento y programa de ordenador correspondiente**

(30) Prioridad:

18.04.2014 FR 1453571

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
03.04.2019

(73) Titular/es:

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

(72) Inventor/es:

NACCACHE, DAVID y
DABBOUS, NORA

(74) Agente/Representante:

ELZABURU, S.L.P

DESCRIPCIÓN

Dispositivo de procesamiento de datos procedentes de una tarjeta inteligente sin contacto, procedimiento y programa de ordenador correspondiente

1. Campo de la invención

El campo de la invención es el del procesamiento de datos sin contacto y más en particular de los terminales que pueden leer tarjetas sin contacto con el fin de realizar operaciones de transacción protegidas.

2. Técnica anterior

En la actualidad existen terminales de comunicación, por ejemplo ordenadores o tabletas, que presentan medios de lectura de tarjetas sin contacto. Para los terminales que no están dotados de tales medios de lectura, existen módulos externos –por ejemplo memorias USB-NFC– que, una vez conectados a un terminal, permiten subsanar esta carencia y realizar operaciones de lectura de tarjetas sin contacto.

Una aplicación corriente de la lectura de tarjetas sin contacto es la realización de una transacción protegida, por ejemplo una operación de pago. Una secuencia clásica de pago sin contacto, puesta en práctica por medio de un terminal de pago, se desarrolla así:

- el usuario presenta su tarjeta inteligente compatible contra el lector sin contacto integrado en el terminal de pago, o contra un lector sin contacto externo conectado al terminal de pago;

- el *software* de a bordo del terminal de pago ejecuta las etapas necesarias para la realización de la transacción. Estas etapas incluyen por ejemplo una petición de introducción del código de identificación personal del usuario, código asociado a su tarjeta sin contacto (por ejemplo código PIN).

- Si es necesario, el usuario introduce su código de identificación personal de identificación y la transacción puede finalizarse (mediante un cálculo de un certificado de transacción resultante de un diálogo entre el terminal de pago y la tarjeta sin contacto).

Para permitir la introducción de este código cuando éste deba ser introducido en el terminal de pago (que por regla general comprende numerosos dispositivos complementarios de protección) pueden aplicarse diferentes medios. Existen medios también para permitir a un usuario evitar tener que introducir este código directamente en el terminal de pago. Así, los documentos US 2011/047036 y US 8151335 describen ambos un dispositivo específico personal del usuario, que puede utilizarse para realizar la introducción del código personal de identificación en el marco de una transacción ejecutada posteriormente por un terminal de pago. Así se refuerza la protección de la introducción, dado que se efectúa en un dispositivo personal del usuario y ya no en un terminal de pago, que por naturaleza es un terminal “público” cuyo funcionamiento ha podido ser alterado por personas maliciosas. En cambio, cuando se desea implementar un pago sin contacto por medio de un terminal de comunicación clásico (de tipo tableta u ordenador, por ejemplo), las soluciones son limitadas. Una primera solución sencilla consiste en permitir al usuario introducir un código secreto en el teclado (del ordenador, de la tableta). Desde el punto de vista de la protección de los datos, esta solución presenta inconvenientes, porque los datos introducidos en el teclado son susceptibles de ser registrados por un *software* de tipo *keylogger* (registrador de teclas). Un *keylogger* es un *software* de espionaje utilizado a menudo con fines maliciosos. Por lo general, ha sido instalado en un terminal a espaldas de su usuario, por ejemplo al abrir un archivo adjunto de aspecto inocuo añadido a un correo electrónico recibido por el usuario. Una vez en marcha, este *software* permite interceptar y transmitir a un tercero las secuencias de teclas pulsadas en el teclado por el usuario, sin que este último sea consciente de ello. Los dispositivos de codificación eventualmente empleados para proteger la información confidencial introducida son ineficaces, dado que el *keylogger* recoge la información en la fuente.

Para defenderse de este fallo de seguridad introducido por los *keyloggers*, una solución alternativa es pedir al usuario que marque su código secreto en un teclado visual mostrado en la pantalla, por medio del ratón o de cualquier otro dispositivo de puntero. Por lo general, la posición de este teclado visual y la disposición de las teclas que lo componen son generadas aleatoriamente en cada uso, con el fin de evitar que un dispositivo malicioso de tipo captura de la posición del ratón pueda permitir a un atacante determinar el código secreto introducido. Sin embargo, esta solución no es completamente fiable, dado que otra categoría de *software* espía está en condiciones de transmitir regularmente y a espaldas del usuario copias de la pantalla de su terminal.

Al estar estos medios de introducción de código (teclado físico, teclado virtual) administrados por el sistema operativo del terminal, están por consiguiente expuestos a ataques potenciales destinados a interceptar datos confidenciales a través de programas maliciosos instalados a espaldas del usuario o mediante la explotación de fallos de seguridad existentes en el *software* instalado. O, para realizar una transacción de pago totalmente protegida en un terminal de comunicación a partir de una tarjeta sin contacto, es absolutamente indispensable garantizar la integridad de la transacción y por lo tanto la ausencia de posibilidad de robo de los datos introducidos por el usuario. Por consiguiente, existe necesidad de proponer una solución que permita asegurar una mejor

protección de las transacciones, en particular durante la introducción de datos confidenciales por un usuario en el marco de la utilización de una tarjeta inteligente sin contacto.

3. Resumen de la invención

El objeto de la invención es un dispositivo que permite realizar la lectura de tarjetas sin contacto –por ejemplo en el marco de una operación de pago– aislando las etapas de adquisición y de restitución de información inherentes a esta transacción con el fin de hacerlas inaccesibles para el sistema operativo del terminal, de manera que un programa malicioso presente en el terminal no pueda acceder a la información confidencial introducida por el usuario durante su operación de pago.

Según la invención, tal dispositivo de lectura de tarjetas sin contacto comprende:

- medios de adquisición de datos de entrada procedentes de un periférico de entrada;

- medios de procesamiento de al menos una secuencia de una transacción inicializada a partir de datos procedentes de una tarjeta sin contacto;

- medios de selección de un modo de funcionamiento, que comprenden al menos dos estados:

  - un estado, denominado estado de inactivación, en el que dichos medios de procesamiento y dicho al menos un lector de tarjetas inteligentes están inactivos;

  - un estado, denominado estado de activación, en el que dichos medios de procesamiento están activos y en el que unos datos de entrada introducidos por medio de dicho periférico de entrada son controlados por dichos medios de procesamiento.

Así, cuando se han de intercambiar datos durante la realización de una transacción, los medios de procesamiento están en condiciones de evitar que los datos introducidos en el periférico de entrada sean interceptados por un módulo de *software* malicioso. En efecto, en el estado de activación del dispositivo, la adquisición y el procesamiento de los datos introducidos son efectuados directamente por el dispositivo. Al ejecutarse estas operaciones fuera del perímetro de acción del sistema operativo, no pueden ser objeto de manipulaciones o de alteraciones por parte de programas maliciosos potencialmente presentes en el terminal.

Según una característica concreta, dicho dispositivo comprende medios de restitución de datos de salida procedentes de dichos medios de procesamiento.

Así, cuando se han de intercambiar datos durante la realización de una transacción, los medios de procesamiento están en condiciones de evitar que los datos restituidos con destino a un periférico de salida sean interceptados, manipulados o alterados por un módulo de *software* malicioso. En efecto, en el estado de activación del dispositivo, los datos restituidos serán visibles sólo para el único usuario que tenga físicamente acceso a dicho periférico de salida.

Según una característica concreta, dicho medio de selección del modo de funcionamiento se presenta en forma de un conmutador.

Así, el usuario tiene la posibilidad de visualizar inmediatamente el modo de funcionamiento en el que se halla el dispositivo y de seleccionar sencillamente otro modo de funcionamiento.

Según una característica concreta, dicho medio de selección del modo de funcionamiento se presenta en forma de una célula de detección de un acontecimiento externo con respecto al dispositivo.

Así, el dispositivo puede ser activado o desactivado sin interacción física del usuario con dicho dispositivo. Así pueden disminuirse las limitaciones de desgaste mecánico y de dimensiones totales del dispositivo.

Según una característica concreta, dichos medios de procesamiento se presentan en forma de un procesador de protección de transacciones financieras.

Así, el dispositivo es apto para utilizarlo para la protección de una operación de pago.

Según una característica concreta, dichos medios de adquisición de datos de entrada procedentes de un periférico de entrada resultan de la aplicación previa de un emparejamiento por *bluetooth* entre dicho dispositivo y dicho periférico de entrada.

Así, la adquisición de los datos de entrada por el dispositivo puede ser efectuada sin necesidad de una conexión por cable entre dicho dispositivo y el periférico de entrada.

Según una característica concreta, dichos medios de adquisición de datos se presentan en forma de un teclado integrado en el dispositivo.

Así, la introducción de los datos puede ser efectuada directamente en el seno del dispositivo, lo que permite utilizarlo junto con terminales de comunicación que no dispongan de periférico de entrada independiente.

Según otro aspecto, la técnica se refiere también a un procedimiento de procesamiento de datos procedentes de una tarjeta inteligente sin contacto. Tal procedimiento comprende:

- una etapa de recepción, por el dispositivo de protección, de un dato de activación;

- una etapa de encaminamiento, por el dispositivo de protección, de al menos un flujo de datos procedente de un dispositivo de entrada de dicho terminal de comunicación, hacia un espacio de memoria de derivación específico de dicho dispositivo de protección;

- una etapa de activación de un mecanismo de aviso a un usuario del dispositivo de comunicación, que suministra una información representativa de un comienzo de transacción;

- una etapa de obtención de al menos un dato procedente de una tarjeta inteligente sin contacto;

- una etapa de realización de una transacción, que comprende una etapa de obtención de datos de entrada a partir de dicho espacio de memoria de derivación específico.

Según una implementación preferida, las diferentes etapas de los procedimientos según la invención son ejecutadas por uno o varios *softwares* o programas de ordenador, que comprenden instrucciones de *software* destinadas a ser ejecutadas por un procesador de datos de un módulo de relevo según la invención y están concebidos para ordenar la ejecución de las diferentes etapas de los procedimientos.

En consecuencia, la invención está dirigida también a un programa que puede ser ejecutado por un ordenador o por un procesador de datos, comprendiendo este programa instrucciones para ordenar la ejecución de las etapas de un procedimiento tal como el anteriormente mencionado.

Este programa puede utilizar cualquier lenguaje de programación y presentarse en forma de código fuente, código de objeto o código intermedio entre el código fuente y el código de objeto, tal como en una forma parcialmente compilada, o en cualquier otra forma deseable.

La invención está dirigida también a un soporte de datos legible por un procesador de datos y que comprende instrucciones de un programa tal como el anteriormente mencionado.

El soporte de datos puede ser cualquier entidad o dispositivo capaz de almacenar el programa. Por ejemplo, el soporte puede comprender un medio de almacenamiento, tal como una ROM, por ejemplo un CD ROM o una ROM de circuito microelectrónico, o también un medio de registro magnético, por ejemplo un disquete (*floppy disc*) o un disco duro.

Por otra parte, el soporte de datos puede ser un soporte transmisible tal como una señal eléctrica u óptica, que puede transportarse a través de un cable eléctrico u óptico, por radio o por otros medios. El programa según la invención puede en particular descargarse en una red de tipo Internet.

Como alternativa, el soporte de datos puede ser un circuito integrado en el que esté incorporado el programa, estando el circuito adaptado para ejecutar el procedimiento en cuestión o ser utilizado en la ejecución del mismo.

Según una forma de realización, la invención se pone en práctica por medio de componentes de *software* y/o materiales. Desde este punto de vista, el término “módulo” puede corresponder en este documento tanto a un componente de *software* como a un componente material o a un conjunto de componentes materiales y de *software*.

Un componente de *software* corresponde a uno o varios programas de ordenador, uno o varios subprogramas de un programa o, de manera más general, a todo elemento de un programa o de un *software* apto para ejecutar una función o un conjunto de funciones, según lo que se describa posteriormente para el módulo afectado. Tal componente de *software* es ejecutado por un procesador de datos de una entidad física (terminal, servidor, pasarela, encaminador (*router*), etc.) y puede acceder a los recursos materiales de esta entidad física (memorias, soportes de registro, bus de comunicación, tarjetas electrónicas de entrada/salida, interfaces de usuario, etc.).

De la misma manera, un componente material corresponde a todo elemento de un conjunto material (o de *hardware*) apto para ejecutar una función o un conjunto de funciones, según lo que se describa posteriormente para el módulo afectado. Puede tratarse de un componente material programable o con procesador integrado para la ejecución de *software*, por ejemplo un circuito integrado, una tarjeta chip, una tarjeta inteligente, una tarjeta electrónica para la ejecución de un *microsoftware* (*firmware*), etc.

Cada componente del sistema previamente descrito ejecuta por supuesto sus propios módulos de *software*.

Las diferentes formas de realización anteriormente mencionadas pueden combinarse entre sí para la puesta en práctica de la invención.

2. Lista de las figuras

Otras características y ventajas de la técnica surgirán más claramente al leer la descripción siguiente de varias formas de realización, ofrecidas a modo de simples ejemplos ilustrativos y no limitativos, y de los dibujos adjuntos, entre los cuales:

- la figura 1 presenta la estructura de un dispositivo de lectura de una tarjeta sin contacto según una primera forma de realización;

- la figura 2 presenta la estructura de un dispositivo de lectura de una tarjeta sin contacto según una segunda forma de realización;

- la figura 3 presenta la estructura de un dispositivo de lectura de una tarjeta sin contacto según una tercera forma de realización;

- la figura 4 ilustra las principales etapas del procedimiento de lectura de una tarjeta sin contacto tal como el ejecutado por el dispositivo descrito;

- la figura 5 ilustra un dispositivo de protección según la técnica propuesta.

5. Descripción de un modo de realización de la técnica

5.1 Principio general

Como se ha expuesto previamente, la técnica propuesta permite proteger la fase de pago a partir de un terminal de comunicación que comprende medios de lectura de datos sin contacto. Estos datos están contenidos en una tarjeta inteligente que dispone de una interfaz de lectura sin contacto. La técnica se refiere a los terminales de comunicación que comprenden medios de comunicación sin contacto, y más en particular a terminales que pueden leer tarjetas sin contacto. La técnica propuesta está relacionada con un dispositivo que permite hacer inaccesibles, para el sistema operativo del terminal, ciertos procesamientos necesarios para la realización de una transacción (estos procesamientos involucran en particular la introducción de información confidencial por parte del usuario). En lo que sigue, este dispositivo se denomina dispositivo de protección de transacciones.

Esto se ha hecho posible integrando, en el dispositivo de protección de transacciones, medios de adquisición de datos, así como medios de procesamiento en condiciones de procesar estos datos sin recurrir al sistema operativo del terminal con el que este dispositivo de protección de transacciones es utilizado. El dispositivo de protección de transacciones comprende además un medio de selección que permite al usuario elegir el modo de funcionamiento deseado. Este medio de selección puede ser físico o de *software*.

En un primer modo de funcionamiento, denominado estado de inactivación, el lector de tarjetas inteligentes sin contacto está inactivado. En este estado, los datos procedentes de los periféricos de entrada no son controlados por el dispositivo de protección de transacciones, que los transmite sin modificación para un procesamiento por el terminal. Los datos introducidos son gestionados al nivel del sistema operativo del terminal, de la misma manera que si dicho dispositivo de protección de transacciones no estuviese presente.

En un segundo modo de funcionamiento, denominado estado de activación, el lector de tarjetas inteligentes está activado. En el marco de la realización de una transacción se solicita la presentación de una tarjeta inteligente sin contacto cerca del lector sin contacto. En este estado, los datos procedentes de al menos un periférico de entrada son interceptados por el dispositivo de protección de transacciones y no son transmitidos al sistema operativo del terminal de comunicación. Los medios de procesamiento integrados en el seno de dicho dispositivo de protección de transacciones son aplicados entonces para controlar todo dato entrante procedente del periférico de entrada controlado.

Así se aumenta la protección de la transacción, los intercambios de datos entre el usuario y el medio de procesamiento integrado en el dispositivo de protección de transacciones no pueden ser interceptados por módulos de *software* maliciosos instalados a espaldas del usuario y que tengan acceso al sistema operativo de su terminal.

Posteriormente se presentan tres formas de realización de un dispositivo de protección de transacciones de este tipo según la técnica propuesta. Sin embargo, está claro que la técnica propuesta no se limita a estas formas de realización concretas, sino que también puede aplicarse en muchas otras formas de realización y, más en general, en todos los casos en los que las ventajas proporcionadas por la técnica propuesta sean de interés.

5.2 Descripciones de formas de realización

Una de las aplicaciones posibles de la presente técnica se refiere a las transacciones bancarias a distancia, y en particular a la protección de la introducción del código de identificación personal necesario para la validación de la transacción por el usuario, después de la utilización de un medio de pago sin contacto, tal como una tarjeta bancaria de pago sin contacto o un teléfono móvil dotado de una tecnología de pago sin contacto.

Cuando un usuario desea efectuar una transacción a distancia con una tarjeta bancaria, por ejemplo a través de Internet, en un sitio comercial, éste solicita información de identificación de la tarjeta bancaria. Esta información se solicita de manera protegida, de forma que no pueda ser utilizada por una persona maliciosa. Esta protección es proporcionada en particular por los sistemas de pago protegido a través de conexiones protegidas, bajo el control de los organismos bancarios.

Tradicionalmente, la información solicitada debe ser introducida por el usuario y es la que figura en la tarjeta bancaria en cuestión, concretamente el número de identificación bancaria de dieciséis cifras, la fecha de caducidad de la tarjeta y un número suplementario de seguridad, denominado criptograma, que por lo general figura en el dorso de la tarjeta.

La introducción de esta información es tediosa, teniendo en cuenta la longitud del número de identificación. También se han desarrollado y promovido soluciones de pago sin contacto para efectuar una transacción a distancia.

El pago sin contacto ya se utiliza para transacciones físicas clásicas, en las instalaciones de los comerciantes equipados con terminales electrónicos de pago compatibles. Para efectuar su compra, el cliente coloca simplemente su tarjeta inteligente sin contacto sobre el terminal de pago, y la transacción se realiza sin otra acción requerida por su parte para los importes relativamente bajos. Para importes mayores se sigue solicitando la introducción de un código de identificación personal.

Aplicado al pago a distancia, por ejemplo a través de Internet, el pago sin contacto permite simplificar la transacción evitando al usuario la necesidad de introducir los números de identificación bancaria, la fecha de caducidad y el criptograma de su tarjeta inteligente. Así, la operación de pago puede efectuarse más rápidamente y se minimiza el riesgo de errores de introducción de datos. Para aumentar la protección de la transacción, puede pedirse al usuario que introduzca un código de identificación personal además de colocar su tarjeta inteligente sin contacto sobre el lector sin contacto de su terminal.

Sin embargo, todo dispositivo de introducción de información administrado por el sistema operativo del terminal presenta un riesgo de interceptación, como se ha explicado previamente.

La presente técnica se refiere a un dispositivo de protección de transacciones que comprende un módulo de lectura de tarjetas sin contacto que permite a un usuario realizar un pago a distancia sin contacto mientras se asegura la protección de la información introducida por el usuario y restituida al usuario haciéndola inaccesible para el sistema operativo del terminal y por consiguiente para el *software* malicioso potencialmente presente en este terminal.

Según una primera forma de realización, ilustrada en la figura 1, el dispositivo (1) de protección de transacciones se utiliza junto con un terminal de comunicación de tipo ordenador de sobremesa, compuesto de una unidad central, de una pantalla y de periféricos de entrada de tipo teclado o ratón. El dispositivo (1) de protección de transacciones está conectado a la unidad central por ejemplo a través de una interfaz, por ejemplo de tipo USB (del inglés *Universal Serial Bus*). El dispositivo (1) de protección de transacciones comprende unos medios (2) de adquisición de datos de entrada, por ejemplo unos puertos USB o PS/2 (del inglés *Personal System/2*) a los que están conectados unos periféricos de entrada de tipo teclado o ratón. El dispositivo (1) de protección de transacciones comprende también un medio (3) de selección, por ejemplo un botón o un conmutador, que permite seleccionar su modo de funcionamiento.

Según una variante, este medio (3) de selección no está físicamente accesible para el usuario en el dispositivo (1) de protección de transacciones, sino que puede estar constituido por una célula de detección interna del dispositivo (1) de protección de transacciones, célula que está en condiciones de detectar un acontecimiento externo de cambio de un estado a otro, por ejemplo la introducción de una combinación concreta de teclas en un periférico de entrada, la recepción de una petición de inicio de una transacción de pago (procedente de un proveedor de servicios de pago por ejemplo).

En un primer modo de funcionamiento, denominado estado de inactivación, el lector de tarjetas inteligentes sin contacto del dispositivo (1) de protección de transacciones está inactivado. En este estado, los datos procedentes de los periféricos de entrada no son controlados por el dispositivo (1) de protección de transacciones, que los transmite sin modificación a la unidad central y por consiguiente al sistema operativo del terminal. Por lo tanto, los datos introducidos son gestionados al nivel del sistema operativo del terminal, de la misma manera que si el dispositivo (1) de protección de transacciones no estuviese presente.

En un segundo modo de funcionamiento, denominado estado de activación, el lector de tarjetas inteligentes del dispositivo (1) de protección de transacciones está activo. Para la realización de una transacción se solicita la presentación de una tarjeta inteligente sin contacto cerca del lector sin contacto. En este estado, los datos procedentes de los periféricos de entrada son interceptados por el dispositivo (1) de protección de transacciones y no son transmitidos al sistema operativo del terminal de comunicación. Los medios de procesamiento (no representados) integrados en el seno del dispositivo (1) de protección de transacciones se aplican entonces para controlar todo dato entrante procedente de los periféricos de entrada, como la introducción de un código de identificación personal por ejemplo. En este segundo modo de funcionamiento, los datos introducidos no se transmiten al sistema operativo. Los datos introducidos se utilizan únicamente para realizar la transacción.

Según una variante de realización, el dispositivo (1) de protección de transacciones comprende además unos medios (4) de restitución de datos de salida, por ejemplo conectores VGA (del inglés *Video Graphics Array*) o puertos HDMI (del inglés *High Definition Multimedia Interface*) o un puerto USB al que estén conectados unos periféricos de salida, por ejemplo una pantalla. En el estado de activación del dispositivo (1) de protección de transacciones, los medios de procesamiento (no representados) integrados en el seno de dicho dispositivo se aplican entonces para generar todo dato de salida con destino al periférico de salida, como la visualización de un teclado visual por ejemplo, que entonces sólo será visible para el único usuario del terminal, dado que esta visualización no es gestionada por el sistema operativo del terminal y escapa por lo tanto a todo intento de interceptación por un *software* malicioso.

Según una segunda forma de realización, ilustrada en la figura 2, el dispositivo (1) de protección de transacciones se utiliza junto con un terminal de comunicación móvil, de tipo tableta o teléfono móvil.

El dispositivo (1) de protección de transacciones está conectado a este terminal por ejemplo por medio de un cable USB.

El dispositivo (1) de protección de transacciones comprende, como para la forma de realización anterior, medios (2) de adquisición de datos de entrada procedentes de un periférico de entrada, medios de procesamiento (no representados) de al menos una secuencia de una transacción inicializada a partir de datos procedentes de una tarjeta sin contacto, medios (3) de selección de un modo de funcionamiento que comprenden al menos dos estados.

Sin embargo, los medios (2) de adquisición de datos de entrada se aplican esta vez a través de una tecnología de comunicación inalámbrica, por ejemplo la tecnología *Bluetooth*. Según esta segunda forma de realización, puede preverse que el dispositivo (1) de protección de transacciones sea apto para emparejarlo a través de *bluetooth* con los periféricos de entrada en una fase de inicialización previa de dicho dispositivo. Según una variante, los medios (2) de adquisición de datos de entrada están integrados en el dispositivo (1) de protección de transacciones. En esta variante, el dispositivo (1) de protección de transacciones comprende un teclado de tipo PINPAD.

Según una tercera forma de realización, ilustrada en la figura 3, el dispositivo (1) de protección de transacciones está totalmente o parcialmente integrado en el terminal de comunicación (integrado en una placa base de un ordenador personal o en una placa base de una tableta o de un teléfono inteligente por ejemplo).

El dispositivo (1) de protección de transacciones comprende, como para la forma de realización anterior, medios (2) de adquisición de datos de entrada procedentes de un periférico de entrada, medios de procesamiento (no representados) de al menos una secuencia de una transacción con datos procedentes de una tarjeta sin contacto, medios (3) de selección de un modo de funcionamiento que comprenden al menos dos estados.

En esta forma de realización, los medios (2) de adquisición pueden presentarse en forma de un teclado autónomo externo con respecto al terminal de comunicación, mientras que los medios de procesamiento (no representados) están integrados en el terminal de comunicación, en forma de un procesador protegido dedicado y de un espacio de memoria dedicado por ejemplo. En el modo de activación del dispositivo (1) de protección de transacciones, es este procesador el que releva al sistema operativo con el fin de interceptar y de controlar los datos entrantes transmitidos por el teclado autónomo y de restituir los datos de salida en el dispositivo de visualización del terminal de comunicación.

Según una cuarta forma de realización, el dispositivo (1) de protección de transacciones está integrado en el terminal de comunicación (integrado en una placa base de un ordenador personal o en una placa base de una tableta por ejemplo). Esta integración se refleja además en la aplicación de al menos un procesador de protección complementario, integrado también en el terminal de comunicación. Tal procesador puede por ejemplo ser un IPT (Identity Protection Technology™ de Intel™). En esta forma de realización concreta, el dispositivo (1) de protección de transacciones comprende una interfaz de control, por medio de comandos concretos, del procesador de protección complementario (PPC). En esta forma de realización, es el procesador de protección complementario el encargado de la interceptación de los datos introducidos por el usuario y de la visualización de los datos protegidos en el dispositivo de visualización. En esta forma de realización, el procesador de protección complementario (PPC) dispone también de una tecnología de gestión de entradas/salidas por codificación. Al recibirse el comando procedente del dispositivo de protección de transacciones, el procesador de protección complementario (PPC) visualiza una ventana de entrada protegida que permite al usuario introducir datos por medio de clics de ratón en lugar de pulsaciones realizadas en el teclado. Cuando el usuario ha introducido la información solicitada, el procesador de protección complementario (PPC) transmite, en forma codificada, al dispositivo de protección de transacciones, el resultado de esta introducción de datos. El dispositivo de protección de transacciones decodifica la información transmitida por medio de su clave privada para verificar la validez de los datos introducidos por el usuario.

Sea cual sea la forma de realización, la técnica requiere una ejecución de la transacción en el seno del dispositivo de protección. Éste es el encargado de la construcción de la transacción y en particular de la creación de un túnel punto a punto con un servidor de transacciones remoto perteneciente a un proveedor de servicios de pago.

A este respecto, el dispositivo de protección comprende por lo tanto, en el seno de una memoria dedicada protegida, material criptográfico utilizado para crear el túnel protegido con el servidor. El material criptográfico puede incluirse en el dispositivo de protección en el momento de la fabricación de éste. El material criptográfico puede también incluirse en una fase ulterior de inicialización.

5.3 Procedimiento de puesta en práctica

A continuación se describe un procedimiento de puesta en práctica de la técnica descrita para realizar una transacción de pago por medio de una tarjeta inteligente sin contacto. El procedimiento comienza después de que el dispositivo haya recibido, del terminal de comunicación o de un servidor comercial al que el terminal de comunicación esté conectado, un importe de transacción (cuando se trate de una transacción de pago) y un beneficiario de la transacción (por ejemplo una cuenta o un identificador bancario). Tal procedimiento comprende:

- una etapa (100) de recepción, por el dispositivo de protección, de un dato de activación (DA); este dato de activación puede recibirse por medio de una petición procedente de un servidor de un proveedor de servicios de pago, o por medio de un botón (*switch*) en el dispositivo de protección mismo o también por medio de una combinación de pulsaciones realizadas en el teclado;

- una etapa (200) de encaminamiento, por el dispositivo de protección, de al menos un flujo (FLX) de datos procedente de un dispositivo de entrada de dicho terminal de comunicación, hacia un espacio (Derv) de memoria de derivación específico de dicho dispositivo de protección;

- una etapa (300) de activación de un mecanismo (AVRT) de aviso a un usuario del dispositivo de comunicación, que suministra una información representativa de un comienzo de transacción; tal información puede presentarse por ejemplo mediante la activación de un diodo luminoso directamente conectado a un procesador del dispositivo de protección o también mediante una visualización específica en la pantalla del terminal de comunicación o también mediante la combinación de estos dos elementos; este mecanismo de aviso inicia un “temporizador” que define un tiempo durante el cual el usuario puede presentar su tarjeta sin contacto delante del lector adecuado;

- una etapa (400) de obtención de al menos un dato (DATAC) procedente de una tarjeta inteligente (CARDM) sin contacto;

- una etapa (500) de realización de una transacción, que comprende una etapa de obtención de datos de entrada a partir de dicho espacio de memoria de derivación específico y dicho al menos un dato de entrada.

Así, el procedimiento propuesto permite realizar una transacción de manera protegida. Los datos de entrada obtenidos a partir del espacio de memoria de derivación específico son por ejemplo un código de identificación personal, que debe ser introducido por el usuario. Este código de identificación personal se solicita en el curso de la realización de la transacción.

5.4 Otras características y ventajas

Se describe, en relación con la figura 5, un dispositivo de protección de pagos que comprende medios que permiten la realización del procedimiento antes descrito.

Por ejemplo, el dispositivo de protección de pagos comprende una memoria 51 formada por una memoria intermedia, una unidad 52 de procesamiento, equipada por ejemplo con un microprocesador, y controlada por el programa 53 de ordenador, que aplica lo necesario para la ejecución de las funciones de pago.

En la inicialización, las instrucciones de código del programa 53 de ordenador son cargadas por ejemplo en una memoria antes de ser ejecutadas por el procesador de la unidad 52 de procesamiento. La unidad 52 de procesamiento recibe en la entrada (E) por ejemplo datos de activación y/o datos representativos de una compra. El microprocesador de la unidad 52 de tratamiento ejecuta las etapas del procedimiento de verificación de autenticidad, según las instrucciones del programa 53 de ordenador para efectuar pagos y notificar en la salida (S) el éxito o el fracaso de estos pagos.

Con este fin, el dispositivo de protección de pagos comprende, además de la memoria intermedia 51, medios de transmisión/recepción de datos sin contacto y eventualmente un procesador de codificación y eventualmente medios de comunicación, tales como módulos de comunicación en red que permitan establecer un enlace protegido punto a punto con un servidor de un proveedor de servicios de pago.

Según la invención, tal dispositivo de protección de pagos comprende además medios de encaminamiento de datos de periféricos de entrada, hacia una memoria de derivación, y medios de lectura de esta memoria de derivación. Estos medios pueden estar controlados por el procesador de la unidad 52 de tratamiento en función del programa 53 de ordenador cuando el dispositivo de protección está activado (sea manualmente, sea electrónicamente). De manera complementaria, tal dispositivo de protección de pagos puede comprender una antena específica, integrada en la carcasa del dispositivo de protección, antena destinada a ponerse en contacto con un módulo de recepción/transmisión sin contacto, por ejemplo presente en una tarjeta inteligente.

REIVINDICACIONES

1. Dispositivo (1) de protección de transacciones para el procesamiento de datos procedentes de una tarjeta inteligente sin contacto, comprendiendo dicho dispositivo al menos un lector de tarjetas inteligentes sin contacto, estando dicho dispositivo conectado o integrado al menos parcialmente en un terminal de comunicación personal de un usuario, estando dicho dispositivo **caracterizado por que** comprende:

- medios (2) de adquisición de datos de entrada procedentes de un periférico de entrada;

- medios de transmisión de dichos datos de entrada a dicho terminal de comunicación;

- medios de procesamiento de al menos una secuencia de una transacción a distancia, inicializada a partir de datos procedentes de una tarjeta sin contacto;

- medios (3) de selección de un modo de funcionamiento, que comprenden al menos dos estados:

  ▪ un estado, denominado estado de inactivación, en el que dichos medios de procesamiento y dicho al menos un lector de tarjetas inteligentes están inactivos, y en el que los datos de entrada introducidos por medio de dicho periférico de entrada son transmitidos a dicho terminal de comunicación mediante dichos medios de transmisión;

  ▪ un estado, denominado estado de activación, en el que dichos medios de procesamiento y dicho al menos un lector de tarjetas inteligentes están activos y en el que unos datos de entrada introducidos por medio de dicho periférico de entrada son controlados por dichos medios de procesamiento.

2. Dispositivo según la reivindicación 1, **caracterizado por que** comprende además medios (4) de restitución de datos de salida procedentes de dichos medios de procesamiento.

3. Dispositivo según la reivindicación 1 o 2, **caracterizado por que** los medios (3) de selección se presentan en forma de un conmutador manipulable por el usuario.

4. Dispositivo según la reivindicación 1 o 2, **caracterizado por que** los medios (3) de selección se presentan en forma de una célula de detección de un acontecimiento externo con respecto al dispositivo.

5. Dispositivo según la reivindicación 1, **caracterizado por que** los medios de procesamiento se presentan en forma de un procesador de protección de transacciones financieras.

6. Dispositivo según la reivindicación 1, **caracterizado por que** los medios (2) de adquisición de datos de entrada procedentes de un periférico de entrada resultan de la aplicación previa de un emparejamiento por *bluetooth* entre dicho dispositivo y dicho periférico de entrada.

7. Dispositivo según la reivindicación 1, **caracterizado por que** dichos medios (2) de adquisición de datos se presentan en forma de un teclado integrado en el dispositivo.

8. Procedimiento de procesamiento de datos procedentes de una tarjeta inteligente sin contacto, mediante un dispositivo de protección de transacciones según la reivindicación 1, comprendiendo dicho dispositivo de protección de transacciones al menos un lector de tarjetas inteligentes sin contacto, estando dicho procedimiento **caracterizado por que** comprende:

- una etapa de recepción, por el dispositivo de protección de transacciones, de un dato de activación;

- una etapa de encaminamiento, por el dispositivo de protección de transacciones, en función de dicho dato de activación, de al menos un flujo de datos procedente de un periférico de entrada de dicho terminal de comunicación, hacia un espacio de memoria de derivación específico de dicho dispositivo de protección de transacciones;

- una etapa de activación de un mecanismo de aviso a un usuario del terminal de comunicación, que suministra una información representativa de un comienzo de transacción;

- una etapa de obtención de al menos un dato procedente de una tarjeta inteligente sin contacto;

- una etapa de realización de una transacción, que comprende una etapa de obtención de datos de entrada a partir de dicho espacio de memoria de derivación específico.

9. Procedimiento según la reivindicación 8, **caracterizado por que** los datos de entrada son un código de identificación personal.

10. Producto de programa de ordenador que puede descargarse desde una red de comunicación y/o almacenarse en un soporte legible por ordenador y/o ejecutarse mediante un microprocesador, **caracterizado por que** comprende instrucciones de código de programa para la ejecución de un procedimiento de procesamiento según la reivindicación 8 cuando es ejecutado en un ordenador.

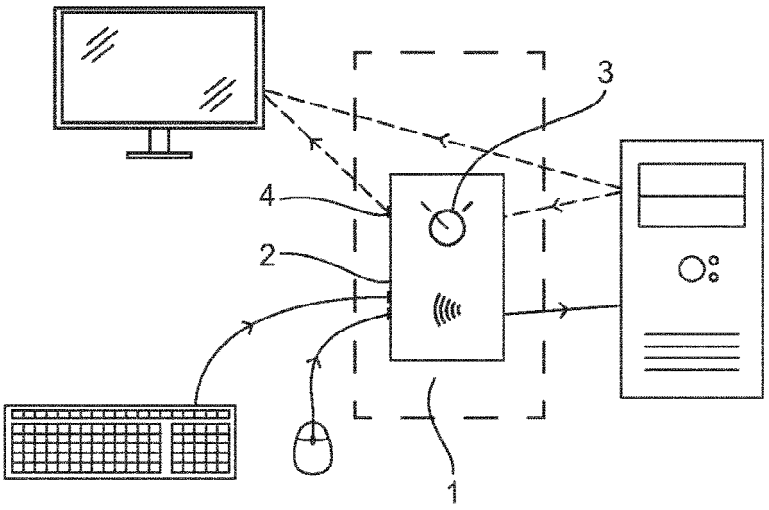

Fig. 1

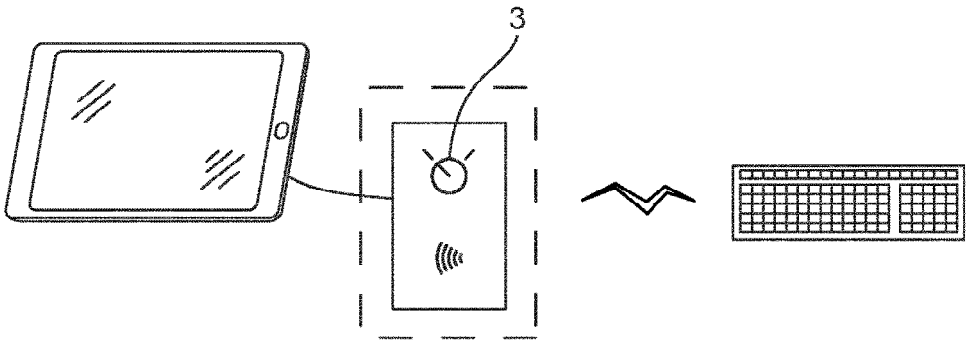

Fig. 2

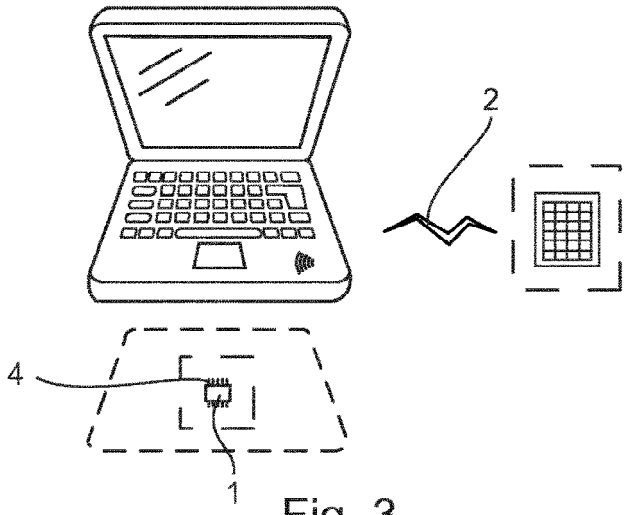

Fig. 3

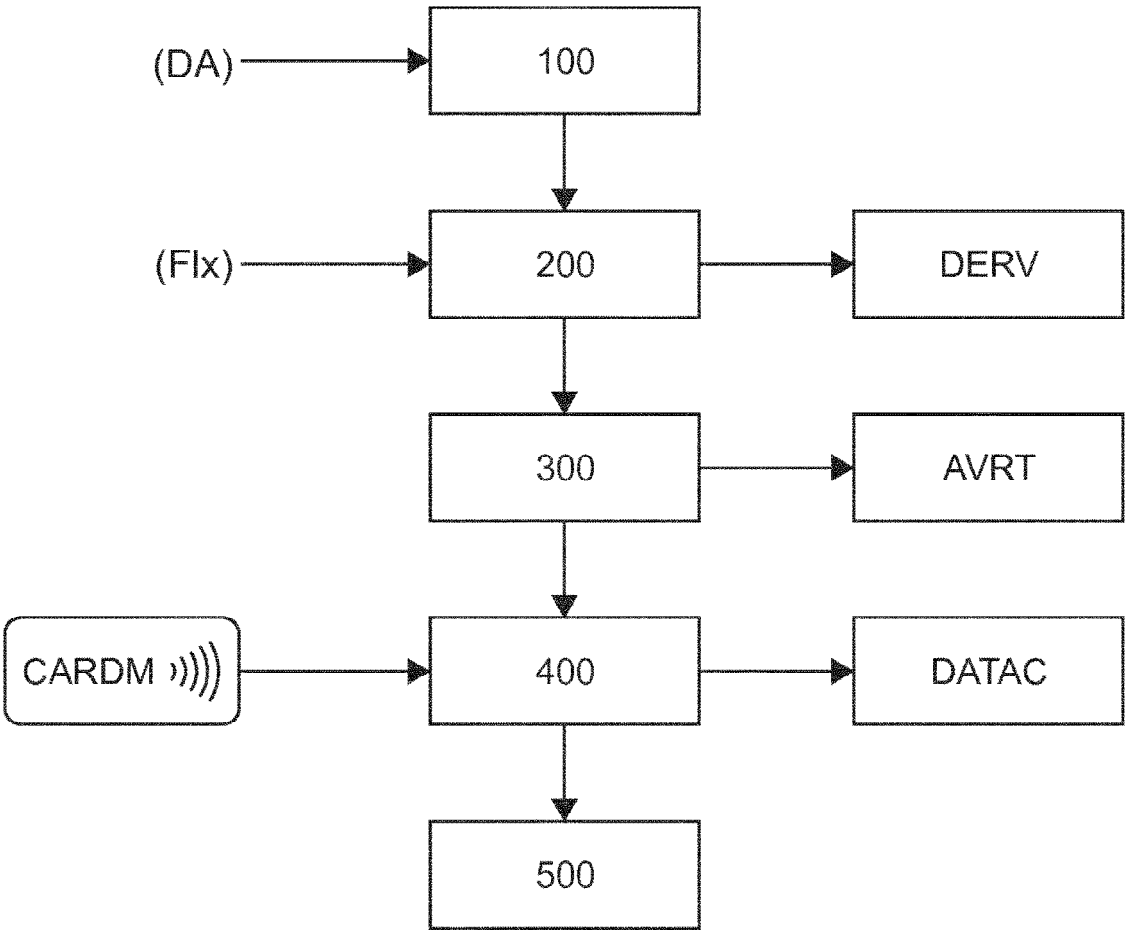
(DA)
100
(FIx)
200
DERV
300
AVRT
CARDM
400
DATAC
500

Fig. 4

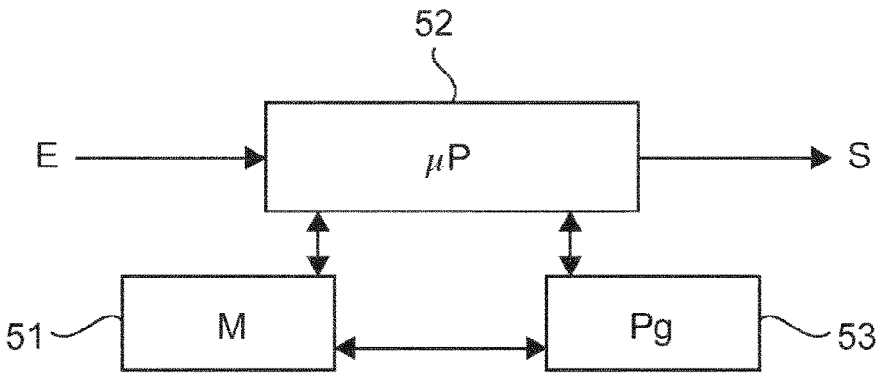
52
E
μP
S
51
M
Pg
53

Fig. 5