(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 643 420**

(51) Int. CI.:

***G07F 7/08*** (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **05.03.2004 E 04290614 (9)**

(97) Fecha y número de publicación de la concesión europea: **12.07.2017 EP 1460593**

(54) Título: **Terminal de pago seguro**

(30) Prioridad:

**18.03.2003 FR 0303297**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
**22.11.2017**

(73) Titular/es:

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

(72) Inventor/es:

**MARDINIAN, GRÉGOIRE y**
**COMPAIN, GÉRARD**

(74) Agente/Representante:

**ELZABURU, S.L.P**

## DESCRIPCIÓN

Terminal de pago seguro

La invención concierne a los sistemas de pago, y de modo más particular a los terminales de pago.

Los sistemas de pago comprenden generalmente cajas o cajas registradoras. A estas cajas están ahora asociadas habitualmente a terminales de pago, que permiten asegurar el pago por tarjeta bancaria. Existen también terminales de pago utilizados independientemente de cualquier caja registradora. Ciertos terminales presentan uno o varios lectores de tarjetas, un visualizador tal como una pantalla LCD y un teclado (o "pin-pad" en lengua inglesa) que permiten al usuario componer y validar un código de identificación personal. Otros terminales no presentan teclado, efectuándose la introducción del código de identificación personal en un periférico distinto. A título de ejemplo, la sociedad Ingenico comercializa con la marca "Elite 510" un terminal fijo, constituido por una primera carcasa con una impresora, una pantalla, un lector de tarjeta, un teclado y una segunda carcasa unida a la primera y que presenta un teclado, una pantalla así como en opción un lector de tarjeta. La segunda carcasa puede ser utilizada por el cliente para la introducción de su código de identificación personal. La sociedad Ingenico comercializa con la marca "Elite 730" un terminal portátil, con una impresora, un lector de tarjeta, un teclado y una pantalla. El terminal comunica por enlace de infrarrojos con su base.

Podrá consultarse el "Manuel de Paiement Electronique" de la Agrupación de tarjetas bancarias para más detalles sobre la estructura y el funcionamiento de tales terminales.

En los terminales de pago existen requisitos de seguridad, para impedir cualquier fraude, como se especifica en las especificaciones VISA SPED. Estos requisitos se refieren al diseño físico de los terminales. Además, en la media en que los terminales pueden aceptar aplicaciones no propias, los requisitos se refieren al diseño de las aplicaciones ejecutadas en estos terminales. En particular, es importante controlar que una aplicación implantada en el terminal después de su entrega por el fabricante no pueda por una visualización en la pantalla del terminal, incitar al usuario a introducir en el teclado su código de identificación personal y a continuación recoger este código.

La figura 1 muestra una vista esquemática de la arquitectura UNICAPT 16 (marca registrada) utilizada por la sociedad Ingenico en los terminales de pago, tales como los terminales Elite 510 y Elite 730 anteriormente mencionados. En la figura 1 se ha representado la parte segura 2 del terminal, que está unida al visualizador 6, al lector de tarjeta 4 y al teclado 8. Esta parte segura 2 es realizada por ejemplo por un componente seguro del tipo del comercializado con la referencia DS5002 por la sociedad DALLAS. Un componente no seguro 10 está unido por un enlace 16 con el protocolo i2c a la parte segura 2 del terminal. Este componente no seguro 10 permite la telecarga de aplicaciones representadas esquemáticamente en 12 en la figura 1, en una memoria 14 del componente 10.

Una aplicación 12 no segura no puede acceder directamente al visualizador y al teclado. En otras palabras, no está permitido a una aplicación no segura dirigirse directamente al visualizador ni recoger directamente del teclado informaciones introducidas por el usuario. Cualquier acceso de la aplicación no segura 12 al visualizador 4 y al teclado 6 se efectúa a través de la parte segura 2 del terminal. De modo más específico, una solución consiste en autorizar a la aplicación no segura 12 a visualizar informaciones en el visualizador 4, pero en bloquear las teclas del teclado cuando tales informaciones sean visualizadas; de este modo, incluso si la aplicación no segura invita al usuario a introducir en el teclado su código de identificación personal, el código introducido por el usuario con el teclado no será trasmitido a la aplicación. Esta solución garantiza la seguridad requerida. La misma sin embargo no permite a una aplicación recoger datos introducidos en el teclado por el usuario.

Otra solución consiste en establecer una firma de las visualizaciones. Las visualizaciones son autorizadas, por ejemplo por el propietario del terminal. La parte segura del terminal puede permitir a una aplicación no segura utilizar el teclado cuando la parte segura constata que la visualización transmitida hacia el visualizador es una visualización autorizada que presenta una firma. Esta solución aumenta el tiempo de desarrollo de las aplicaciones; cualquier modificación de una aplicación no segura implica obtener nuevas firmas de las visualizaciones. Esta solución está descrita en el documento US-A-5 493 613 o en el documento US-A-6 226 749.

Existe por tanto una necesidad de un terminal de pago, que satisfaga los requisitos de seguridad, pero que sin embargo permita la implantación simple y la ejecución de aplicaciones.

La invención por tanto propone, en un modo de realización, un terminal de pago, que presenta un teclado, un visualizador y un lector de tarjeta, un primer software adaptado para gobernar el teclado, el visualizador y el lector de tarjeta, un segundo software adaptado para acceder al teclado y al visualizador por intermedio del primer software, estando adaptado el primer software para restringir el acceso del segundo software al teclado o al visualizador en cuanto una tarjeta sea recibida en el lector de tarjeta.

Se puede también prever que el terminal presente una o varias de las características siguientes:

- el primer software está adaptado para restringir el acceso del segundo software al teclado y al visualizador en cuanto una tarjeta sea recibida en el lector de tarjeta;

- el primer software está adaptado para restringir el acceso del segundo software al teclado o al visualizador en cuanto una tarjeta que contenga una aplicación dada sea recibida en el lector de tarjeta;
- el primer software está adaptado para restringir el acceso del segundo software al teclado o al visualizador en cuanto una aplicación dada de la tarjeta sea seleccionada por el terminal;
- el terminal presenta un estado no seguro en el cual el segundo software accede libremente al teclado y al visualizador;
- el terminal pasa al estado no seguro a la expiración de una duración tras la recepción de una tarjeta en el lector;
- el terminal pasa al estado no seguro cuando una tarjeta es retirada del lector,
- el terminal pasa al estado no seguro cuando el primer software reconoce la introducción en el teclado de un código de identificación personal;
- el teclado presenta una tecla de validación y el terminal pasa al estado no seguro cuando la tecla de validación es accionada;
- en el estado no seguro, el segundo software accede libremente al lector de tarjeta.

La invención propone todavía un procedimiento de explotación de un terminal de pago que presenta un teclado, un visualizador y un lector de tarjeta, un primer software adaptado para gobernar el teclado, el visualizador y el lector de tarjeta, y un segundo software adaptado para acceder al teclado y al visualizador por intermedio del primer software; el procedimiento comprende una etapa de restricción por el primer software del acceso del segundo software al teclado o al visualizador en cuando una tarjeta sea recibida en el lector de tarjeta.

El procedimiento puede comprender una etapa de lectura de la tarjeta recibida en el lector, restringiendo el primer software el acceso del segundo software al teclado o al visualizador cuando una aplicación dada sea leída en la tarjeta.

El procedimiento puede comprender todavía una etapa de selección de una aplicación de la tarjeta por el terminal, restringiendo el primer software el acceso del segundo software al teclado o al visualizador cuando una aplicación dada sea seleccionada por el terminal.

El procedimiento puede igualmente comprender una etapa de liberación del acceso del segundo software al teclado y al visualizador.

Otras características y ventajas de la invención se pondrán de manifiesto en la lectura de la descripción detallada que sigue de los modos de realización de la invención, dados únicamente a título de ejemplo y refiriéndose a los dibujos, que muestran:

- figura 1, una vista esquemática de la arquitectura de un terminal del estado de la técnica;
- figura 2, una vista esquemática de la arquitectura lógica de un terminal de acuerdo con la invención;
- figura 3, un diagrama de estado del terminal de la figura 2.

La invención propone un terminal de pago, que funciona según un modo seguro y según un modo no seguro. El terminal presenta un software seguro que gobierna el teclado, la pantalla y el lector de tarjeta del terminal. El mismo presenta también un software no seguro que accede al teclado y al visualizador a través del primer software. En un modo seguro, el software seguro restringe el acceso del software no seguro al teclado o al visualizador. El terminal pasa al modo seguro en cuanto una tarjeta sea recibida en el lector. Así, el terminal es seguro, pero permite también la ejecución de aplicaciones nos seguras.

La figura 2 muestra una vista esquemática de la arquitectura lógica de un terminal de acuerdo con la invención. En la figura se ha representado el controlador de teclado 20, el controlador de visualizador 22 y el controlador de lector 24. Los softwares ejecutados en el terminal comprenden un software seguro, representado en 26 en la figura 2; se trata típicamente del software implantado de origen por el fabricante del terminal. El software seguro 26 dirige los diferentes controladores, como está representado en la figura 2 por trazos continuos que unen el software seguro 26 y los controladores 20, 22 y 24. La representación de la figura 2 es una representación de la arquitectura de software y hablando en propiedad, el software dirige los controladores 20, 22 y 24. Por abuso de lenguaje, se dice también que el software dirige la pantalla, el visualizador o el teclado, aunque hay una interfaz de software que es el controlador correspondiente.

Los softwares ejecutados en el terminal comprenden también un software no seguro, representado en 28 en la figura 2. Puede tratarse por ejemplo de un software telecargado por el usuario del terminal. El software no seguro dirige los controladores de teclado y de visualizador 20 y 22 por intermedio del software seguro 26, como está representado

en la figura 2 por trazos interrumpidos que unen el software no seguro 28 a los controladores 20 y 22 a través del software seguro 26.

El terminal presenta al menos dos modos de funcionamiento, como representa el diagrama de estado de la figura 3. En un modo seguro 30, el software seguro 26 restringe el acceso del software no seguro al controlador de teclado 20, al controlador de visualizador 22 o a los dos. La restricción depende del nivel de seguridad deseado; se puede dejar visualizar mensajes en el visualizador pero bloquear la introducción en el teclado; se puede también impedir la visualización en el visualizador al tiempo que se autorice la introducción en el teclado. Se puede finalmente impedir al software no seguro cualquier acceso al teclado y al visualizador. En una aplicación con un código de identificación personal, puede ser suficiente bloquear el acceso de un software no seguro al teclado para impedir que este software pueda recoger un código introducido por un usuario; se puede también impedir el acceso del software no seguro a la pantalla para evitar cualquier invitación al usuario para que el mismo introduzca su código.

El terminal presenta un segundo modo de funcionamiento 32, calificado de modo no seguro. En este modo no seguro, el software no seguro 28 dirige libremente el controlador de teclado 20 y el controlador de visualizador 22. Esto permite a una aplicación dirigirse libremente al visualizador y al teclado, sin limitaciones particulares en el desarrollo de la aplicación. El desarrollo de la aplicación o su modificación puede efectuarse por tanto de modo más simple que en el estado de la técnica.

El terminal pasa del modo no seguro al modo seguro en cuanto una tarjeta sea recibida en el lector, como está representado por la flecha 34 en la figura 2. En el caso de un lector de tarjeta con memoria, el paso del modo no seguro al modo seguro puede efectuarse desde la detección de la presencia de una tarjeta en el lector; se puede también pasar del modo no seguro al modo seguro en cuanto el protocolo de lectura de la memoria de la tarjeta con memoria haya reconocido una tarjeta válida. En el caso de un lector de pista magnética, el paso del modo no seguro al modo seguro puede tener lugar en cuanto una pista sea leída por el lector. Si el terminal presenta varios lectores de tarjeta – de tipos diferentes o del mismo tipo – el paso del modo no seguro al modo seguro puede tener lugar en cuanto una tarjeta sea leída en uno de los lectores.

El paso del modo no seguro al modo seguro puede igualmente tener lugar cuando una tarjeta que contenga al menos una aplicación específica dada sea leída en el lector.

Así, el primer software seguro 26 está adaptado para restringir el acceso del segundo software no seguro 28 al teclado o al visualizador según el tipo de tarjeta insertada en el lector de tarjeta o según el tipo de aplicación seleccionada en la tarjeta. Las tarjetas pueden en efecto contener varias aplicaciones diferentes que el terminal puede seleccionar. Por aplicación, se entienden softwares o repertorios embarcados en la tarjeta, tales como softwares (repertorios) de pago de tipo débito, de crédito, de fidelidad, de repertorios, etc…

Así, si una tarjeta que contenga una aplicación bancaria es introducida en el lector de tarjeta, el primer software puede restringir el acceso del segundo software al teclado y al visualizador. Si una tarjeta contiene simplemente una aplicación de fidelidad de cliente, el primer software puede restringir solo el acceso al teclado y permitir la visualización. El protocolo de lectura de tarjeta lee la memoria de la tarjeta introducida en el lector de tarjeta y puede identificar el tipo de aplicación contenido en la tarjeta. Esta lectura es interpretada por el primer software que entonces adapta en función la restricción de acceso del segundo software al teclado o al visualizador. La restricción puede ser adaptada solamente después de la selección por el terminal de una de las aplicaciones de la tarjeta.

El paso al modo seguro cuando es recibida una tarjeta en el lector garantiza la seguridad: una aplicación no segura no puede invitar al portador de una tarjeta a introducir su código de identificación personal cuando la tarjeta está en el terminal, ni recoger este código. En la medida en que los usuarios sepan que el código de identificación personal solo debe ser introducido en el teclado cuando la tarjeta está en el lector, el terminal de pago es seguro.

El paso de modo seguro 30 al modo no seguro 32 puede efectuarse de diferentes modos. En el ejemplo de la figura 3, se ha representado el paso por la flecha 36, cuando la tarjeta es retirada del lector. Esta solución está adaptada especialmente a lectores de tarjeta con memoria. La misma asegura que en tanto que la tarjeta esté en el lector, el terminal permanece en el modo seguro. Se puede también prever que el terminal pase al modo seguro después del reconocimiento por el software seguro de un código de identificación personal. En este caso, la seguridad reposa en la hipótesis de que el usuario no introduce dos veces seguidas su código de identificación personal. Se puede también prever que el teclado presente una tecla de validación y que el terminal pase al modo no seguro después de una validación desde el teclado; en este caso, la seguridad reposa en la hipótesis de que cualquier introducción del código de identificación personal va seguida de una validación desde el teclado. Esto equivale a pasar del modo seguro al modo no seguro en una acción sobre una tecla dada del teclado. Se podría también pasar al modo no seguro cuando se active en el teclado una secuencia de teclas (y no solamente una sola tecla). Se podría también pasar al modo no seguro a la expiración de una duración (fija o programable) después del paso al modo seguro; esto deja el interrogante del tiempo para que el software seguro recoja el código de identificación personal. De modo más general, el paso del modo seguro al modo no seguro depende del nivel de seguridad deseado y de las hipótesis de comportamientos del portador de la tarjeta.

En el encendido, se puede arrancar el terminal en uno o el otro de los modos. Se puede especialmente arrancar en modo seguro y pasar al modo no seguro si se constata que el lector no contiene tarjeta. Esta solución evita eventuales problemas en caso de arranque con una tarjeta introducida en el lector.

El terminal de las figuras 2 y 3 permite una gran libertad en el diseño, el desarrollo o la modificación de las aplicaciones no propietarias o no seguras. El mismo sin embargo asegura un nivel de seguridad elevado.

Desde el punto de vista del hardware, el terminal de las figuras 2 y 3 puede ser realizado de cualquier modo. Se puede utilizar una arquitectura de hardware semejante a la de la figura 1, pero cualquier otra arquitectura de hardware es posible. La seguridad del terminal puede basarse únicamente en soluciones de software, descritas en la figura 2, o también en una combinación de medios de software y de hardware.

Naturalmente, la presente invención no está limitada a los modos de realización descritos a título de ejemplo; así, se pueden prever más estados que los mostrados en la figura 3. Se puede también prever que el cambio de estado del terminal se efectúe de otro modo que el representado en la figura 3. Así, se podría pasar de nuevo al modo no seguro tras la lectura de una tarjeta y después de haber identificado que la tarjeta no es una tarjeta protegida; esta solución permitirá la utilización del terminal para la lectura y la escritura en tarjetas gestionadas por el software no seguro 28 y no serían necesariamente reconocidas por el software seguro. Se puede prever, especialmente en este caso, que el software no seguro pueda también dirigir el control de lector 24 en el modo no seguro.

Se pueden prever todavía como en el estado de la técnica, soluciones de firma de las visualizaciones. Dicho de otro modo, la restricción puesta en práctica por el software seguro no es necesariamente como en el ejemplo una prohibición total, sino que puede basarse en un mecanismo de firma o de autorización.

**Lista de referencias**

| | |
|---|---|
| 2 | parte segura |
| 4 | visualizador |
| 6 | lector de tarjeta |
| 8 | teclado |
| 10 | componente no seguro |
| 12 | aplicación |
| 14 | memoria del componente no seguro |
| 16 | conexión |
| 20 | control teclado |
| 22 | control visualizador |
| 24 | control lector |
| 26 | software seguro |
| 28 | software no seguro |
| 30 | modo seguro |
| 32 | modo no seguro |
| 34 | lectura de tarjeta |
| 36 | retirada de tarjeta |

**REIVINDICACIONES**

1. Un terminal de pago, que presenta un teclado (20), un visualizador (22) y un lector de tarjeta (24), un primer software (26) adaptado para controlar el teclado (20), el visualizador (22) y el lector de tarjeta (24), un segundo software (28) adaptado para acceder al teclado (20) y al visualizador (22) por intermedio del primer software, presentando el citado terminal al menos los dos estados siguientes:

- un estado no seguro en el cual el segundo software accede libremente al teclado y al visualizador;
- un estado seguro en el cual el acceso del segundo software al teclado o al visualizador está prohibido o sometido a un mecanismo de autorización por el primer software;

y estando caracterizado el citado terminal por que el mismo pone en práctica medios de detección de la presencia de una tarjeta en el citado lector de tarjeta, pasando la citada detección de la presencia de una tarjeta en el citado lector de tarjeta el citado terminal del citado estado no seguro al citado estado.

2. El terminal de la reivindicación 1, caracterizado por que, en el citado estado seguro, el acceso del segundo software al teclado o al visualizador está prohibido o sometido a un mecanismo de autorización por el primer software cuando una aplicación dada es identificada en la memoria leída de la tarjeta detectada en el lector de tarjeta.

3. El terminal de la reivindicación 2, caracterizado por que, en el citado estado seguro, el acceso del segundo software al teclado o al visualizador está prohibido o sometido a un mecanismo de autorización por el primer software cuando la citada aplicación dada identificada en la citada memoria de la citada tarjeta detectada en el lector de tarjeta es seleccionada por el terminal.

4. El terminal de la reivindicación 1, caracterizado por que el terminal pasa al estado no seguro a la expiración de una duración después de la citada detección de la presencia de la citada tarjeta en el lector.

5. El terminal de la reivindicación 1, caracterizado por que el terminal pasa al estado no seguro cuando la citada tarjeta es retirada del lector.

6. El terminal de la reivindicación 1, caracterizado por que el terminal pasa al estado no seguro cuando el primer software reconoce la introducción en el teclado de un código de identificación personal.

7. El terminal de la reivindicación 1, caracterizado por que el teclado presenta una tecla de validación y por que el terminal pasa al estado no seguro cuando la tecla de validación es accionada.

8. El terminal de la reivindicación 1, caracterizado por que en el estado no seguro, el segundo software accede libremente al lector de tarjeta.

9. Un procedimiento de explotación de un terminal de pago que presenta un teclado (20), un visualizador (22) y un lector de tarjeta (24), un primer software (26) adaptado para controlar el teclado (20), el visualizador (22) y el lector de tarjeta (24), un segundo software (28) adaptado para acceder al teclado (20) y al visualizador (22) por intermedio del primer software, cuyo primer software permite restringir el acceso al teclado o al visualizador del segundo software en un estado seguro, caracterizado por que el procedimiento comprende:

- una etapa de detección de la presencia de una tarjeta en el lector de tarjeta, haciendo pasar la citada detección de la presencia de una tarjeta en el lector de tarjeta el citado terminal desde un estado no seguro al citado estado seguro.

10. El procedimiento de la reivindicación 9, caracterizado por que el mismo comprende una etapa de lectura de la memoria de la tarjeta detectada en el lector y por que la citada etapa de prohibición o de sumisión a un mecanismo de autorización por el primer software del acceso del segundo software al teclado o al visualizador es puesta en práctica cuando una aplicación dada es identificada en la citada memoria leída de la tarjeta.

11. El procedimiento de la reivindicación 10, caracterizado por que el mismo comprende una etapa de selección de una aplicación de la tarjeta por el terminal y por que la citada etapa de prohibición o de sumisión a un mecanismo de autorización por el primer software del acceso del segundo software al teclado o al visualizador es puesta en práctica cuando la citada aplicación dada identificada en la citada memoria leída de la tarjeta es seleccionada por el terminal.

12. El procedimiento de una de las reivindicaciones 9 a 11, caracterizado por que el mismo comprende una etapa de acceso libre del segundo software al teclado y al visualizador.

FIG_1

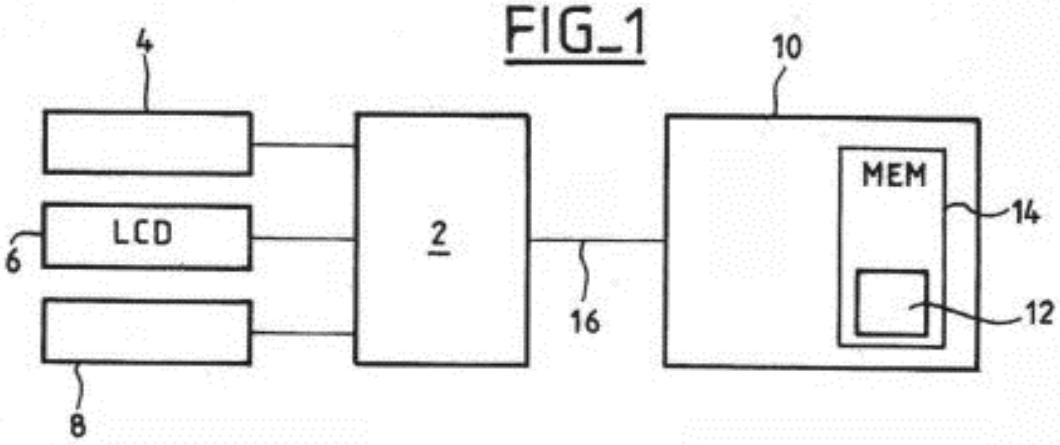


FIG_2

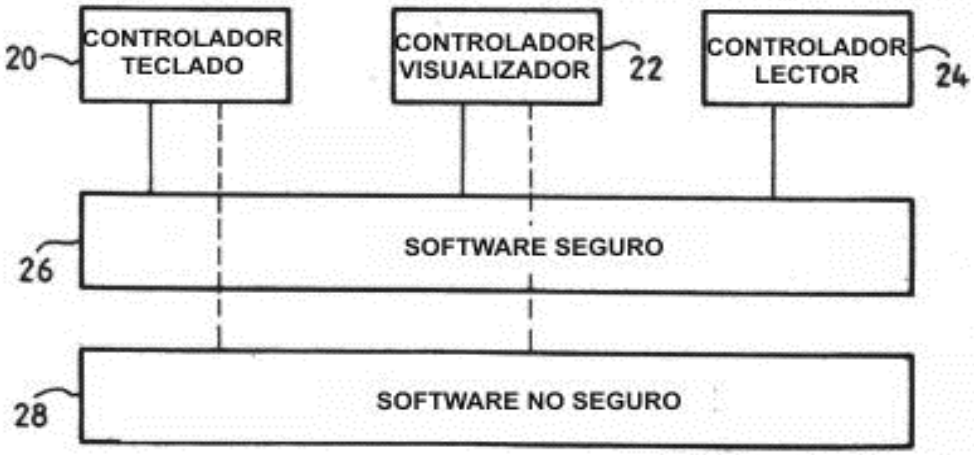


FIG_3