(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 725 786**

(51) Int. CI.:

G06F 21/44 (2013.01)
G06F 21/60 (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **18.12.2012 PCT/FR2012/052979**

(87) Fecha y número de publicación internacional: **27.06.2013 WO13093330**

(96) Fecha de presentación y número de la solicitud europea: **18.12.2012 E 12819091 (5)**

(97) Fecha y número de publicación de la concesión europea: **20.02.2019 EP 2795524**

(54) Título: **Procedimiento y dispositivo de aseguramiento de una aplicación informática**

(30) Prioridad:

20.12.2011 FR 1162036

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
27.09.2019

(73) Titular/es:

ORANGE (100.0%)
78, rue Olivier de Serres
75015 Paris, FR

(72) Inventor/es:

ASSADI, HOUSSEM;
HABERMACHER, LOÏC y
LOUET, ERWAN

(74) Agente/Representante:

ISERN JARA, Jorge

DESCRIPCIÓN

Procedimiento y dispositivo de aseguramiento de una aplicación informática

Antecedentes de la invención

La presente invención se sitúa en el campo del aseguramiento de una aplicación informática que se ejecuta en un terminal.

Más precisamente, la invención se sitúa en el campo del aseguramiento de aplicaciones informáticas que solicitan la introducción de datos sensibles de un usuario, por ejemplo una contraseña o un código secreto.

La aplicación informática en cuestión se crea por un suministrador de aplicaciones. La invención está dirigida a impedir que una aplicación fraudulenta creada por un tercero malintencionado, obtenga dichos datos en el momento en que se introducen por el usuario.

En este contexto, se ha identificado un problema particular en el que una aplicación fraudulenta introducida en el terminal sin el conocimiento del usuario se ejecuta en segundo plano sobre el terminal y superpone sobre la pantalla de introducción de la aplicación pirateada, una pantalla de introducción fraudulenta, copia exacta de esta pantalla de introducción, para recuperar los datos introducidos por el usuario.

En el estado actual de la técnica, se conocen unos mecanismos de aseguramiento que se dirigen a combinar la pantalla de introducción de los datos sensibles con una imagen conocida por el usuario.

Desgraciadamente el aseguramiento propuesto por este mecanismo no es suficiente porque el suministrador de aplicaciones no puede garantizar la autenticidad de esta imagen conocida. La solicitud de patente FR2893732 A1 divulga un procedimiento que permite al usuario autentificar un sistema de confianza interactuando con él a través de su interfaz y que atribuye un carácter dinámico a los datos de autentificación. Los criterios de autentificación comprenden no solamente unos datos estáticos sino también unos datos debidos al comportamiento, es decir respuestas esperadas del sistema como reacción a unos eventos desencadenados por el usuario.

La patente americana US6.950.949 B1 divulga un método que emite una información de legitimidad de la interfaz de entrada de naturaleza dinámica y que permite al usuario determinar de manera visual o auditiva si una interfaz de entrada es legítima o no.

La invención propone un procedimiento de aseguramiento y un terminal que implementa este procedimiento que corrige ciertos fallos del procedimiento de la técnica anterior mencionado anteriormente.

Objeto y sumario de la invención

Más precisamente, la invención se refiere a un procedimiento de aseguramiento de una aplicación informática que se ejecuta en un terminal tal como se define por la reivindicación independiente 1, un programa informático según la reivindicación 8 y un soporte de registro según la reivindicación 10.

Correlativamente, la invención se refiere a un dispositivo de aseguramiento de una aplicación informática que se ejecuta sobre un terminal tal como se ha definido por la reivindicación independiente 12.

De esa forma, y de manera general, la invención propone, como la técnica de la técnica anterior anteriormente mencionada, presentar sobre la pantalla del terminal, una imagen conocida por el usuario de este terminal, para reforzar su confianza sobre el hecho de que la aplicación informática que se ejecuta en el terminal es una aplicación autorizada.

De manera notable, contrariamente a la técnica anterior, el archivo binario que representa la imagen secreta conocida por el usuario, se memoriza en un elemento de seguridad del terminal. Este elemento de seguridad puede estar constituido por ejemplo por una tarjeta SIM, un soporte extraíble de tipo "Secure SD Card" o un elemento de seguridad integrado en el terminal ("Embedded Secure Element") o también una zona asegurada del procesador de aplicación gracias a la utilización de una tecnología de seguridad integrada en el procesador (por ejemplo la tecnología TrustZone, marca registrada de la compañía ARM).

De ese modo, al memorizar la imagen secreta en el elemento de seguridad, se hace muy difícil, para una aplicación fraudulenta, obtener este fichero binario para crear una pantalla fraudulenta. La invención garantiza la autenticidad de la imagen secreta.

Por otra parte, contrariamente a la técnica anterior, la imagen presentada sobre la pantalla del terminal no es la simple imagen secreta conocida por el usuario, sino una imagen compleja obtenida a partir de esta imagen secreta y de un dato dinámico inaccesible para el terminal. El hecho de combinar la imagen secreta con un dato dinámico (dicho de

otra manera de "variabilizar" la imagen secreta) aumenta considerablemente la entropía de la imagen presentada sobre la pantalla del terminal, con lo que incluso si una aplicación fraudulenta lograra obtener copia de la imagen presentada, podría muy difícilmente reconstruir la imagen secreta para engañar al usuario.

La invención se aplica en particular para aplicaciones de pago sin contacto, por ejemplo de acuerdo con la norma NFC.

En este contexto particular de implementación de la invención, el dato dinámico puede ser un montante de la transacción de pago.

De una manera general, es preferible que el dato dinámico sea un parámetro de la aplicación a asegurar.

De acuerdo con la invención, el dato dinámico es inaccesible para el terminal. Esto significa que las aplicaciones del terminal no pueden obtener este dato dinámico en tanto que tal, sino simplemente la imagen de estos datos dinámicos combinada con la imagen secreta.

De acuerdo con la invención, el procedimiento de aseguramiento se implementa cuando se detecta que la aplicación a asegurar se apresta para invitar al usuario del terminal a introducir unos datos.

Esta invitación puede hacerse de diferentes maneras.

Por ejemplo, la invitación puede ser un mensaje de audio que invite al usuario a introducir unos datos de manera vocal.

En este caso, a partir de que se detecte este mensaje de audio, se presenta la imagen compleja sobre la pantalla del terminal.

En un modo particular de la invención, la invitación se realiza por una pantalla de la aplicación que incluye una zona de introducción de texto de los datos.

En este modo de realización, el aseguramiento consiste en combinar la imagen compleja con esta pantalla de aplicación.

Se acerca así a la solución de la técnica anterior pero, con dos diferencias principales, según las que:

- por una parte la imagen secreta se memoriza en un elemento de seguridad del terminal; y
- por otra parte, la imagen secreta se combina con un dato dinámico inaccesible para el terminal.

La invención puede implementarse para asegurar unas aplicaciones en las que los datos introducidos por el usuario se validan de manera implícita.

Por ejemplo, la invención puede implementarse en un procedimiento en el que se solicita al usuario introducir un código secreto de cuatro cifras, validando la introducción de la 4ª cifra la introducción del código secreto.

Pero la invención, se aplica preferentemente para aplicaciones en las que se solicita al usuario validar la introducción de manera explícita.

En este modo de realización, la presentación se efectúa antes de permitir la validación de la introducción.

Se puede solicitar así al usuario confirmar que la imagen compleja presentada sobre la pantalla del terminal corresponde a la imagen secreta elegida por este usuario.

Se puede esperar así a una confirmación de ese tipo antes de presentar al usuario unos botones de validación de la introducción.

Pueden concebirse dos variantes principales de la invención.

Según una primera variante, la aplicación a asegurar incluye por sí misma los medios para obtener la imagen secreta, para constituir la imagen compleja y para presentar esta imagen compleja sobre la pantalla del terminal.

En este modo de realización de la invención, es necesario que la aplicación pueda acceder al elemento de seguridad para obtener la imagen secreta y para constituir la imagen compleja.

Pero no es indispensable, para la implementación de este modo de realización, que la aplicación se ejecute en sí misma en el elemento de seguridad.

En una segunda variante de realización, la invención puede implementarse mediante una aplicación de aseguramiento con el fin de asegurar otra aplicación informática.

Es simplemente necesario, en esta variante de realización, que la aplicación de aseguramiento pueda obtener un mensaje de la aplicación informática a asegurar según el que se prepara para invitar al usuario a introducir unos datos.

La aplicación de aseguramiento constituye entonces la imagen compleja y la reenvía a la aplicación a asegurar que la presenta en la pantalla. Si, a continuación de esta presentación, el usuario confirma haber reconocido la imagen secreta, la validación de la introducción puede hacerse mediante una acción del usuario.

Una aplicación de ese tipo de aseguramiento se ejecutará preferentemente en el elemento de seguridad.

En un modo particular de realización de la invención, la aplicación a asegurar se ejecuta al menos parcialmente en el elemento de seguridad. Este es particularmente el caso para una aplicación de pago, en la que se ejecuta en el terminal un módulo de interfaz hombre-máquina, el módulo encargado del pago propiamente dicho se ejecuta en el elemento de seguridad.

En un modo particular de realización, las diferentes etapas del procedimiento de aseguramiento se determinan mediante unas instrucciones de programas informáticos.

En consecuencia, la invención también tiene como propósito un programa de ordenador sobre un soporte de informaciones, siendo susceptible este programa de ser implementado en un ordenador, incluyendo este programa instrucciones adaptadas para la implementación de las etapas del procedimiento de aseguramiento tal como se ha mencionado anteriormente.

En un modo particular de la invención, este programa incluye además instrucciones para ejecutar al menos una parte de la aplicación informática a asegurar.

Este programa puede utilizar no importa qué lenguaje de programación, y estar en la forma de código fuente, código objeto o código intermedio entre código fuente y código objeto, tal como en una forma parcialmente compilada o en cualquier otra forma deseable.

La invención también tiene como propósito un soporte de informaciones legible por un ordenador y que incluye unas instrucciones de un programa de ordenador tal como se ha mencionado más arriba.

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

Pueden concebirse diferentes soluciones.

Por ejemplo, el soporte de registro incluye:

- un programa informático adecuado para implementar el procedimiento de aseguramiento según la invención, pero no la aplicación a asegurar; o
- un programa informático adecuado para implementar la aplicación a asegurar y el procedimiento según la invención; o
- dos programas informáticos independientes; uno para implementar la aplicación informática a asegurar, el otro para implementar el procedimiento según la invención.

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

De manera alternativa, el soporte de informaciones puede ser un circuito integrado en el cual se incorpora el programa, estando el circuito adaptado para ejecutar o para ser utilizado en la ejecución del procedimiento en cuestión.

La invención se dirige igualmente a un elemento de seguridad que incluye un dispositivo tal como se ha mencionado anteriormente.

En un modo particular de realización, el elemento de seguridad según la invención incluye un campo de seguridad accesible únicamente por la aplicación informática a asegurar, memorizándose el archivo binario en el campo de seguridad. La noción de campo de seguridad es por ejemplo la propuesta por la norma Global Platform e implementada normalmente en los elementos de seguridad tales como las tarjetas SIM/USIM de nueva generación.

Esto permite reforzar la seguridad de la solución, principalmente cuando el elemento de seguridad incluye varias aplicaciones informáticas, teniendo cada una acceso a su propia imagen secreta de manera estanca.

La invención se dirige igualmente a un terminal que incluye un dispositivo tal como se ha mencionado anteriormente o un elemento de seguridad tal como se ha mencionado anteriormente.

En un modo particular de realización, el terminal según la invención incluye además unos medios, por ejemplo el sistema operativo del terminal, adecuados para impedir copias de la pantalla del terminal.

Este modo de realización es particularmente ventajoso, porque permite igualmente asegurar unas aplicaciones contra ataques de aplicaciones fraudulentas que estarían en condiciones de detectar la presentación de la imagen compleja según la invención y crear sobre la marcha una copia de acuerdo con esta imagen para obtener fraudulentamente los datos introducidos por el usuario.

Breve descripción de los dibujos

Surgirán otras características y ventajas de la presente invención de la descripción realizada a continuación con referencia a los dibujos que ilustra en ellos un ejemplo de realización desprovisto de todo carácter limitativo.

En las figuras:

- la figura 1 representa una pantalla de aplicación de una aplicación que puede asegurarse por la invención;
- las figuras 2A y 2B representan una imagen secreta y una imagen compleja en el sentido de la invención;
- las figuras 3A y 3B representan unas pantallas de aplicaciones aseguradas por la invención;
- la figura 4 representa un terminal de acuerdo con un modo particular de realización de la invención; y
- la figura 5, representa, en forma de organigrama, las principales etapas del procedimiento de aseguramiento de acuerdo con un modo particular de realización de la invención.

Descripción detallada de la invención

La figura 1 representa una pantalla de aplicación EA de una aplicación que puede ser asegurada por la invención.

Esta pantalla de aplicación incluye una zona de introducción ZS en la que el usuario puede, por ejemplo, introducir un código secreto y dos botones B1 y B2 para validar o anular la introducción de los datos en la zona ZS.

La figura 2A representa una imagen secreta IMS en el sentido de la invención. Se trata de la imagen elegida por el usuario del terminal, estando destinada esta imagen a ser memorizada en un elemento de seguridad del terminal.

La figura 2B representa una imagen compleja en el sentido de la invención.

Esta imagen compleja se obtiene por combinación de la imagen secreta de la figura 2A y de un dato dinámico inaccesible para el terminal.

En este ejemplo, la aplicación informática a asegurar es una aplicación de pago y el dato dinámico es un montante (10 €) de una transacción que el usuario se apresta a validar mediante la introducción de un código secreto.

De manera general, un dato dinámico depende de la aplicación implementada en el terminal móvil. Este es un dato volátil que es apropiado para la ejecución actual de la aplicación. El ejemplo dado aquí es un montante de la transacción, en el marco de una aplicación de pago. La invención no está por supuesto limitada a este ejemplo de dato dinámico. De ese modo, en otro ejemplo de realización, el dato dinámico es una foto del bien a comprar, una característica del bien a comprar cuyo usuario puede conocer independientemente de una lectura por medio de su terminal móvil, una foto del vendedor, si está enfrente de él, etc.

La figura 3A representa la pantalla de aplicación de la figura 1 combinada con la imagen compleja IMC de la figura 2B.

Esta pantalla está destinada a ser presentada al usuario para la introducción de los datos.

El usuario reconoce entonces su imagen secreta IMS y se asegura por tanto de la conformidad de la aplicación que presenta esta pantalla.

De acuerdo con la invención, esta imagen secreta IMS se combina con el dato dinámico constituido en este caso por el montante de la transacción, tan bien que es muy difícil para una aplicación fraudulenta reconstituir esta imagen compleja. En el ejemplo presentado en relación con la figura 2B, la combinación de la imagen secreta con el dato dinámico consiste en una superposición del dato dinámico sobre la imagen secreta. En otros ejemplos de realización, la combinación consiste en presentar lado con lado el dato dinámico y la imagen secreta o en presentar alternativamente en la pantalla en un período de tiempo corto del orden del segundo la imagen secreta y el dato

dinámico. De manera general, puede concebirse cualquier combinación del dato dinámico con la imagen secreta, a partir del momento en que el usuario percibe en esta imagen compleja la presencia del dato dinámico y de su imagen secreta.

En el ejemplo de la figura 3A, se presenta al usuario un "check box" CB para solicitarle confirmar que ha reconocido correctamente la imagen compleja IMS antes de presentarle los botones de validación de la introducción.

La pantalla de la aplicación que incluye sus botones de validación se presenta en la figura 3B.

La figura 4 representa un terminal TRM de acuerdo con la invención.

Este terminal incluye:

- una pantalla DSP;
- un procesador 21 adecuado para implementar las funciones clásicas de un terminal de comunicaciones;
- una memoria volátil de tipo RAM 22;
- una memoria no volátil de tipo ROM 23 que incluye, en este ejemplo, un sistema operativo OS, un programa P2 ejecutado por el procesador 21 para implementar las funciones clásicas del terminal y un módulo IHM de la aplicación a asegurar APP, realizando este módulo IHM la interfaz entre el usuario y el módulo de seguridad MS de esta aplicación;
- un elemento de seguridad SEC constituido en este caso por una tarjeta SIM; y
- un módulo de comunicación NFC ("Near Field Communication"), permitiendo particularmente este módulo de comunicación al terminal efectuar unas transacciones de pago con un lector no representado. Más precisamente, este módulo de comunicación permite intercambios de datos, constituyendo estos intercambios las transacciones, entre el lector, o terminal sin contacto, y una aplicación instalada en el módulo de seguridad.

El elemento asegurado SEC incluye en este caso un procesador 11, una memoria de tipo RAM 12 y una memoria no volátil de tipo ROM 13.

Esta memoria no volátil de tipo ROM 13 constituye un soporte en el sentido de la invención. Incluye el módulo asegurado MS de la aplicación APP a asegurar y un programa informático P1 de acuerdo con la invención. Este programa informático incluye instrucciones para permitir la ejecución de las etapas del procedimiento de aseguramiento según la invención que se describirá posteriormente con referencia a la figura 5.

De acuerdo con la invención, el elemento de aseguramiento incluye igualmente un archivo binario que incluye la imagen secreta IMS de la figura 2A.

En el modo de realización descrito en este caso, Este archivo binario se memoriza en un campo de seguridad DS propio de la aplicación APP.

El elemento de seguridad SEC incluye igualmente un bus para recibir datos de transacciones y principalmente unos montantes de la transacción. Más precisamente, estos montantes se reciben directamente del terminal sin contacto en el transcurso de una transacción. En particular, no transitan por una memoria del terminal TRM. En este sentido, estos montantes, que constituyen los datos dinámicos son inaccesibles para el terminal TER.

Estos montantes de la transacción constituyen unos datos dinámicos adecuados para combinarse con la imagen de seguridad IMS para presentación al usuario del terminal.

Con referencia a la figura 5, se describirá ahora un modo particular de realización de la invención.

En el curso de una etapa E10, el procesador 11 del elemento de seguridad SEC obtiene una información según la que la aplicación APP se apresta a invitar al usuario del terminal TRM a introducir unos datos.

Esta etapa puede consistir en recibir un mensaje particular del módulo asegurado MS de la aplicación de pago APP.

En el curso de una etapa E20, el procesador 11 accede al archivo binario memorizado en el elemento de seguridad DS para obtener la imagen secreta IMS conocida por el usuario del terminal.

En el curso de una etapa E30, el procesador 11 combina esta imagen secreta IMS con unos datos dinámicos DD correspondientes al montante de la transacción. Se observará que los datos dinámicos DD no salen jamás del elemento asegurado SEC. En efecto, los datos dinámicos DD se han recibido por medio del módulo NFC que los ha comunicado directamente al campo de seguridad DS en el que la aplicación P1 los ha aprovechado. Simplemente se combinan, en forma de imagen con la imagen secreta IMS para constituir una imagen compleja IMC.

La imagen compleja IMC se presenta al usuario en el transcurso de una etapa E40. Esta imagen compleja se combina, en este ejemplo, con la pantalla de aplicación EA de la aplicación APP como se ha representado en la figura 3A.

Si el usuario marca la "check box" CB, interpretándose esta operación como el hecho de que el usuario ha reconocido la imagen secreta IMS, se le presentan los botones B1 y B2 de validación o anulación de la introducción como se ha representado en la figura 3B.

Se supone que el usuario valida la introducción de los datos secretos en el transcurso de una etapa E50.

En el modo de realización descrito en este caso, en el curso de una etapa E60, se verifica si la imagen de seguridad IMS ha sido leída, un número MAX predeterminado de veces.

Si tal es el caso, se invita al usuario, en el curso de una etapa E70, a cambiar la imagen secreta memorizada en el campo de seguridad DS.

El procesador 11, las memorias 12 y 13 y el programa informático P1 constituyen un ejemplo de dispositivos de aseguramiento en el sentido de la invención, para asegurar la aplicación informática APP, porque ofrecen:

- unos medios para obtener una información según la que la aplicación APP se apresta a invitar a un usuario del terminal TRM a introducir unos datos;
- unos medios de acceso a un archivo binario representativo de una imagen secreta conocida por el usuario del terminal, memorizándose este archivo binario en un elemento de seguridad del terminal;
- unos medios para constituir, en el elemento de seguridad, una imagen compleja obtenida a partir de la imagen secreta y de un dato dinámico inaccesible para dicho terminal; y
- unos medios para presentar esta imagen compleja sobre una pantalla del terminal.

REIVINDICACIONES

1. Procedimiento de aseguramiento de una aplicación informática (APP) que se ejecuta en un terminal (TRM) que comprende una pantalla (DSP) y un elemento de seguridad (SEC), incluyendo este procedimiento:

- una etapa (E10) de obtención, por parte del elemento de seguridad (SEC), de una información según la que dicha aplicación se apresta a invitar a un usuario del terminal a introducir unos datos;
- una etapa (E20) de acceso, por parte del elemento de seguridad (SEC), a un archivo binario representativo de una imagen secreta conocida para el usuario del terminal, memorizándose este archivo binario en el elemento de seguridad (SEC) del terminal;
- una etapa (E30) para constituir, en dicho elemento de seguridad, una imagen compleja obtenida por combinación de dicha imagen secreta y de un dato dinámico que no sale jamás del elemento de seguridad y por tanto inaccesible a dicho terminal; y
- una etapa (E40) para presentar dicha imagen compleja sobre la pantalla (DSP) del terminal.

2. Procedimiento de aseguramiento según la reivindicación 1 caracterizado por que dicha presentación (E40) se efectúa antes de la validación (E50) de dicha introducción.

3. Procedimiento de aseguramiento según la reivindicación 1, en el que dicha invitación consiste en presentar una pantalla de aplicación que incluye una zona de introducción (ZS) de dichos datos, caracterizado por que dicha etapa de presentación (E40) consiste en presentar una imagen obtenida por combinación, en el seno de dicho elemento de seguridad, de dicha pantalla de aplicación (EA) con dicha imagen compleja (IMC).

4. Procedimiento de aseguramiento según la reivindicación 1, caracterizado por que incluye una etapa (E70) para incitar al usuario a cambiar dicha imagen secreta.

5. Procedimiento de aseguramiento según la reivindicación 1, caracterizado por que dicha aplicación (APP) se ejecuta al menos parcialmente en dicho elemento de seguridad (SEC).

6. Procedimiento de aseguramiento según la reivindicación 1, caracterizado por que dicho dato dinámico (DD) es un parámetro de dicha aplicación.

7. Procedimiento de aseguramiento según la reivindicación 6, caracterizado por que, dicha aplicación es una aplicación de pago sin contacto, dicho dato dinámico es el montante de una transacción.

8. Programa informático (P1) que incluye instrucciones para la ejecución de cada una de las etapas del procedimiento de aseguramiento según una cualquiera de las reivindicaciones 1 a 7, cuando dicho programa se ejecuta por un procesador (11).

9. Programa informático según la reivindicación 8, caracterizado por que incluye además instrucciones para ejecutar al menos una parte (MS) de dicha aplicación informática cuando dicho programa se ejecuta por dicho procesador.

10. Soporte de registro (13) legible por un ordenador en el que se registra un programa informático según la reivindicación 8 o 9.

11. Soporte de registro según la reivindicación 10, caracterizado por que incluye un primer programa (PM) según la reivindicación 9 y un segundo programa, independiente de dicho primer programa, incluyendo este segundo programa instrucciones para ejecutar al menos una parte (MS) de dicha aplicación informática (APP) cuando dicho programa se ejecuta por un procesador (L11).

12. Terminal (TRM) configurado para ejecutar una aplicación informática (APP), comprendiendo dicho terminal una pantalla (DSP) y un elemento de seguridad (SEC); incluyendo dicho elemento de seguridad (SEC):

- unos medios de obtención de una información según la que dicha aplicación se apresta a invitar a un usuario del terminal a introducir unos datos;
- unos medios de acceso a un archivo binario representativo de una imagen secreta conocida por el usuario del terminal, memorizándose este archivo binario en un elemento de seguridad (SEL) del terminal;
- unos medios para constituir, en dicho elemento de seguridad, una imagen compleja obtenida por combinación de dicha imagen secreta y de un dato dinámico que no sale jamás del elemento de seguridad y por tanto inaccesible a dicho terminal; y
- unos medios para presentar dicha imagen compleja sobre una pantalla del terminal.

13. Terminal según la reivindicación 12, caracterizado por que el elemento de seguridad (SEC) incluye un campo de seguridad (DS) propio de dicha aplicación informática (APP), memorizándose dicho archivo binario en el campo de seguridad.

14. Terminal según la reivindicación 12, caracterizado por que incluye unos medios adecuados para impedir las copias de pantallas de dicho terminal.

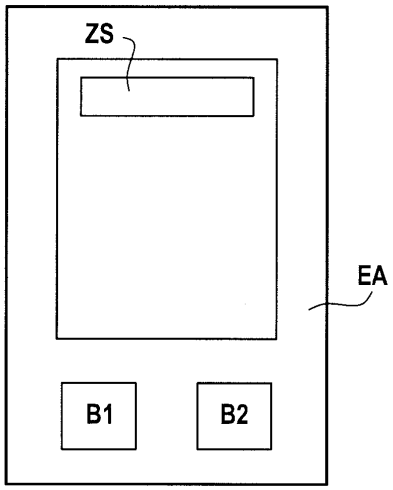

FIG.1

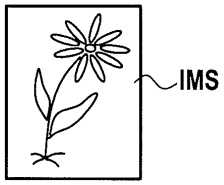

FIG.2A

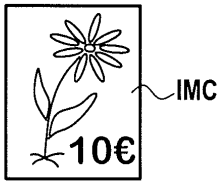

FIG.2B

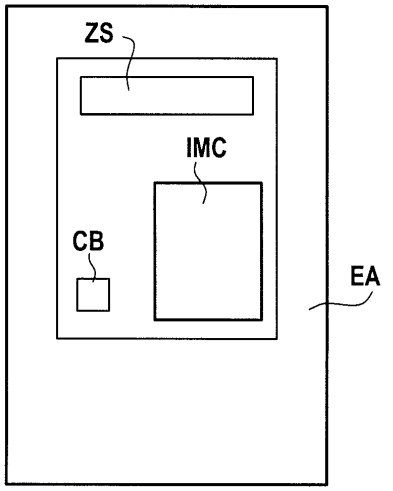

FIG.3A

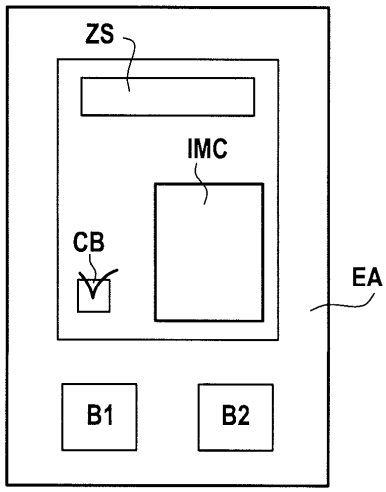

FIG.3B

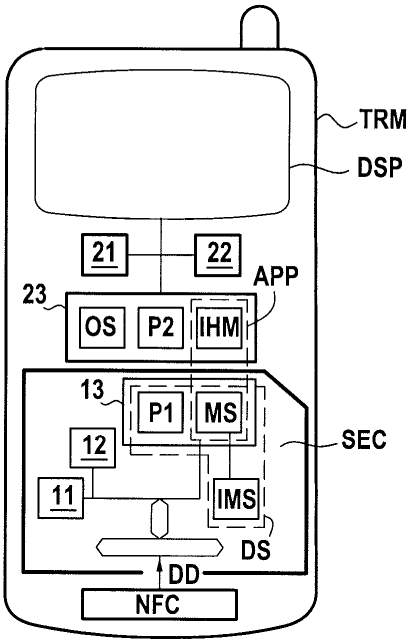
TRM
DSP
21
22
APP
23
OS
P2
IHM
13
P1
MS
SEC
12
11
IMS
DS
DD
NFC

FIG.4

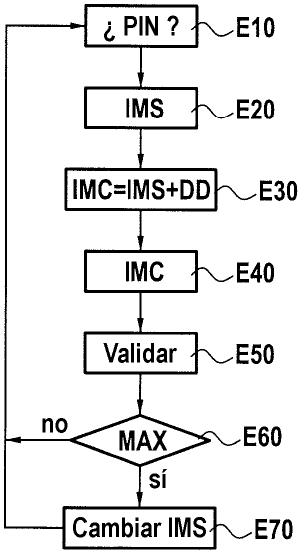
¿ PIN ?
E10
IMS
E20
IMC=IMS+DD
E30
IMC
E40
Validar
E50
no
MAX
E60
sí
Cambiar IMS
E70

FIG.5