(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 875 609**

(51) Int. CI.:

G06F 21/32 (2013.01)
G06Q 40/02 (2012.01)
G06Q 20/10 (2012.01)
G06Q 20/40 (2012.01)
G07F 7/10 (2006.01)
G06Q 20/34 (2012.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **07.03.2017 E 17159649 (7)**

(97) Fecha y número de publicación de la concesión europea: **28.04.2021 EP 3208731**

(54) Título: **Método y dispositivo de configuración de un dispositivo para realizar operaciones bancarias**

(30) Prioridad:

17.02.2016 FR 1651276

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
10.11.2021

(73) Titular/es:

IDEMIA IDENTITY & SECURITY FRANCE (100.0%)
2, Place Samuel de Champlain
92400 Courbevoie, FR

(72) Inventor/es:

GESLAIN, RAPHAËL;
DAILLE-LEFEVRE, DAVID y
PEPIN, CYRILLE

(74) Agente/Representante:

ELZABURU, S.L.P

DESCRIPCIÓN

Método y dispositivo de configuración de un dispositivo para realizar operaciones bancarias

La presente invención se refiere a un método y a un dispositivo de configuración de un dispositivo para realizar operaciones bancarias en los que se utilizan los datos biométricos del usuario del dispositivo para realizar operaciones bancarias para autenticar al usuario del dispositivo para realizar operaciones bancarias.

Hoy en día, en el ámbito de los elementos de seguridad, es posible permitir el almacenamiento y a continuación la verificación de los datos biométricos con fines de autentificación, lo que permite la apertura de diversos derechos, en particular en el ámbito del cruce de fronteras.

Los datos biométricos son, por ejemplo, al menos una huella dactilar y/o datos representativos de rasgos faciales y/o reconocimiento del iris y/o huella vocal.

Sin embargo, actualmente no existe ningún medio implementado dentro de un elemento seguro con el fin de que permita dichas operaciones biométricas con fines transaccionales o de operaciones bancarias, en particular no existe ningún medio de autentificación biométrica que sea totalmente compatible además con las normas aplicadas a las tarjetas de pago, tal como la norma EMV.

EMV es una norma internacional para las tarjetas de débito o de crédito con chip iniciada por el consorcio EMVCo. Proporciona un nivel de seguridad mucho mayor en comparación con las tarjetas con banda y se basa en gran medida en la tarjeta con chip original.

En la actualidad, los métodos de autentificación del portador de un dispositivo para realizar operaciones bancarias, tal como una tarjeta bancaria, se basan en un sistema de código confidencial. En caso de pérdida o de robo de la tarjeta, cuando un tercero ha logrado obtener el código confidencial de la tarjeta bancaria, éste puede sustituir a placer al titular original del medio de pago.

El portador o usuario original, por ejemplo, para el caso de una tarjeta bancaria, es el cliente al que el banco emite la tarjeta después de su personalización, así como de un código confidencial tal como el PIN.

El código confidencial contiene de cuatro a doce dígitos, se personaliza en los datos ligados con la aplicación presente dentro de la tarjeta con chip y se comunica al usuario de dicha tarjeta con chip con el fin de que se autentifique junto con la tarjeta.

Los terceros siempre tienen una oportunidad del número total de combinaciones de diferentes códigos para encontrar la correcta por casualidad, es decir, una oportunidad entre diez mil cuando el PIN consta de cuatro dígitos El documento WO 2010/022129 se considera como un estado de la técnica anterior para la presente invención.

La presente invención se define mediante las reivindicaciones independientes 1, 9 y 11 y tiene por objetivo resolver los inconvenientes de la técnica anterior proponiendo un método y un dispositivo para realizar operaciones bancarias que garanticen a su usuario que sólo él se podrá autenticar en el dispositivo para realizar operaciones bancarias con el fin de autorizar una transacción bancaria. Además, la presente invención tiene por objetivo introducir, en un dispositivo para realizar operaciones bancarias, medios de autentificación biométrica que sigan siendo compatibles con las normas del sector, en particular la norma EMV.

Para ello, de acuerdo con un primer aspecto, la invención proporciona un método de configuración y utilización de un dispositivo para realizar operaciones bancarias en el que se utilizan datos biométricos del usuario del dispositivo para realizar operaciones bancarias para autenticar al usuario del dispositivo para realizar operaciones bancarias, caracterizado por que el método incluye las etapas de:

- activación de varias órdenes a partir de identificadores de una norma relativa a las transacciones bancarias disponibles para la realización de órdenes no predefinidas por la norma,

- creación, a partir de un identificador de la norma relativa a las transacciones bancarias disponible para la realización de órdenes no predefinidas por la norma, en el dispositivo para realizar operaciones bancarias, de un contenedor que pueda almacenar datos biométricos de referencia de un usuario del dispositivo para realizar operaciones bancarias,

- memorización de los datos biométricos de referencia, a partir de un identificador de la norma relativa a las transacciones bancarias disponible para la realización de órdenes no predefinidas por la norma, en el contenedor de datos biométricos de referencia del usuario del dispositivo para realizar operaciones bancarias,

La presente invención también se refiere a un dispositivo para realizar operaciones bancarias en el que se utilizan los datos biométricos del titular del dispositivo para realizar operaciones bancarias para autenticar al usuario del dispositivo para realizar operaciones bancarias, caracterizado por que el dispositivo incluye:

- medios de activación de varias órdenes a partir de identificadores de una norma relativa a las transacciones bancarias disponibles para la realización de órdenes no predefinidas por la norma,

- medios de creación, a partir de un identificador de la norma relativa a las transacciones bancarias disponible para la realización de órdenes no predefinidas por la norma, en el dispositivo para realizar operaciones bancarias, de un contenedor capaz de almacenar los datos biométricos de referencia de un usuario del dispositivo para realizar operaciones bancarias,

- medios de memorización de los datos biométricos de referencia, a partir de un identificador de la norma relativa a las transacciones bancarias disponible para la realización de órdenes no predefinidas por la norma, en el contenedor de datos biométricos de referencia del usuario del dispositivo para realizar operaciones bancarias.

De este modo, la autentificación del usuario del dispositivo para realizar operaciones bancarias con el fin de autorizar una transacción bancaria es más fiable.

Además, el dispositivo para realizar operaciones bancarias de acuerdo con la presente invención sigue siendo compatible con las normas del sector, en particular con la norma EMV.

De acuerdo con una forma de realización particular de la invención, el método incluye, además, antes de las etapas de activación, creación y memorización, la etapa de activación o no, en el dispositivo para realizar operaciones bancarias, de la funcionalidad de datos biométricos para autenticar al usuario del dispositivo para realizar operaciones bancarias.

De este modo, el diseño del dispositivo para realizar operaciones bancarias permite su utilización en un sistema convencional de autentificación con código confidencial o en un sistema en el que se implemente la presente invención.

De acuerdo con una forma de realización particular de la invención, el método incluye además las etapas de:

- recepción de los datos biométricos candidatos para una operación bancaria,

- comparación de los datos biométricos candidatos con los datos biométricos de referencia,

- autorización o rechazo de la transacción bancaria en función de la comparación.

De acuerdo con una forma de realización particular de la invención, el método incluye además la etapa de memorización, en el dispositivo para realizar operaciones bancarias, de instrucciones capaces de procesar al menos una de las siguientes órdenes: verificación de los datos biométricos sin encriptación, verificación de los datos biométricos con encriptación, desbloqueo de un contador de errores, lectura de un contador de errores.

De este modo, la autentificación del usuario del dispositivo se puede llevar a cabo siguiendo diferentes métodos a elección del emisor del dispositivo, y se puede adjuntar un contador de errores al contenedor con el fin de seguir la evolución del número de datos biométricos candidatos erróneos en comparación con los datos biométricos de referencia.

De acuerdo con una forma de realización particular de la invención, el método incluye además la etapa de memorización en el dispositivo para realizar operaciones bancarias, de instrucciones adecuadas para procesar el registro de datos biométricos después de que el dispositivo para realizar operaciones bancarias haya sido proporcionado a su usuario.

De este modo, es posible para el usuario, con el dispositivo para realizar operaciones bancarias en su poder, registrar los datos biométricos de su elección dentro del dispositivo para realizar operaciones bancarias y esto en un entorno seguro.

De acuerdo con una forma de realización particular de la invención, en caso de rechazo de la transacción bancaria, el método incluye además la etapa del incremento de un contador de rechazos.

De este modo, de acuerdo con esta forma de realización particular de la invención, es posible seguir la evolución del número de datos biométricos candidatos erróneos en comparación con los datos biométricos de referencia.

De acuerdo con una forma de realización particular de la invención, el método incluye además las etapas de comparación del valor del contador de rechazos con un valor predeterminado y, si el valor del contador de rechazos es igual al valor predeterminado, seleccionar otro modo de autentificación del usuario del dispositivo y, si es necesario, rechazar cualquier operación bancaria mientras el contador de rechazos no se haya actualizado.

De este modo, la utilización correcta del dispositivo para realizar operaciones bancarias de acuerdo con esta forma de realización particular de la invención está condicionada a la presentación de datos biométricos candidatos válidos, y la presentación de un valor límite predeterminado de datos candidatos no válidos bloquea este método de autentificación del portador del dispositivo para realizar operaciones bancarias.

De acuerdo con una forma de realización particular de la invención, cuando se actualiza el contador de rechazos, el método incluye además la etapa de actualizar en el contenedor nuevos datos biométricos de referencia del usuario del dispositivo para realizar operaciones bancarias.

De este modo, es posible reintroducir los datos biométricos de referencia dentro de un entorno seguro, con el fin de permitir al titular del dispositivo almacenar datos biométricos que le permitan autenticarse, si por casualidad los datos biométricos de referencia anteriores han sido capturados de forma incorrecta.

De acuerdo con una forma de realización particular de la invención, si la funcionalidad no está habilitada, el método incluye las etapas de:

- recepción de un código de autentificación candidato para una operación bancaria,

- comparación del código de autentificación candidato con un código de referencia memorizado en el dispositivo para realizar operaciones bancarias,

- autorización o rechazo de la transacción bancaria en función de la comparación del código de autentificación candidato con el código de referencia.

De este modo, si la funcionalidad no está habilitada dentro del dispositivo para realizar operaciones bancarias, dicho dispositivo para realizar operaciones bancarias cumple con las normas que rigen el entorno tecnológico de dicho dispositivo para realizar operaciones bancarias.

De acuerdo con una forma de realización particular de la invención, el dispositivo para realizar operaciones bancarias es una tarjeta con chip o está incluido en un teléfono móvil.

De este modo, el usuario de dicha tarjeta con chip se puede autenticar en dicha tarjeta con chip durante cada transacción bancaria utilizando sus datos biométricos candidatos.

La invención también se refiere a programas de ordenador almacenados en un soporte de información, incluyendo dichos programas, instrucciones que permiten llevar a cabo los métodos descritos anteriormente cuando son cargados y ejecutados por un sistema informático.

Las características de la invención mencionadas anteriormente, así como otras, parecerán más claras con la lectura de la siguiente descripción de un ejemplo de forma de realización, siendo realizada dicha descripción en relación con los dibujos adjuntos, de los cuales:

la Fig. 1 muestra un sistema de configuración y/o utilización de un dispositivo para realizar operaciones bancarias en el que se utilizan los datos biométricos del titular del dispositivo para realizar operaciones bancarias para autorizar o rechazar un pago de acuerdo con la presente invención;

la Fig. 2 muestra un ejemplo de la arquitectura de un dispositivo para realizar operaciones bancarias de acuerdo con la presente invención;

la Fig. 3 muestra un ejemplo de la arquitectura de un dispositivo de configuración de un dispositivo para realizar operaciones bancarias de acuerdo con la presente invención;

la Fig. 4 muestra un ejemplo de módulos de software implementados en el dispositivo para realizar operaciones bancarias de acuerdo con la presente invención;

la Fig. 5 muestra un ejemplo de un algoritmo ejecutado por un dispositivo de configuración de un dispositivo para realizar operaciones bancarias de acuerdo con una primera forma de realización de la presente invención;

la Fig. 6 muestra un ejemplo de un algoritmo ejecutado por un dispositivo de configuración de un dispositivo para realizar operaciones bancarias de acuerdo con una segunda forma de realización de la presente invención;

la Fig. 7a muestra un ejemplo de un algoritmo ejecutado por un dispositivo de configuración de un dispositivo para realizar operaciones bancarias de acuerdo con la segunda forma de realización de la presente invención;

la Fig. 7b muestra un ejemplo de un algoritmo ejecutado por un dispositivo de configuración de un dispositivo para realizar operaciones bancarias de acuerdo con la presente invención;

la Fig. 8 muestra un ejemplo de un algoritmo ejecutado por un dispositivo para realizar operaciones bancarias de acuerdo con la presente invención.

La Fig. 1 muestra un sistema de configuración y/o utilización de un dispositivo para realizar operaciones bancarias en el que se utilizan los datos biométricos del titular del dispositivo para realizar operaciones bancarias para autorizar o rechazar un pago de acuerdo con la presente invención.

El sistema de configuración y/o utilización de un dispositivo para realizar operaciones bancarias 10a o 10b en el que se utilizan los datos biométricos del titular o usuario del dispositivo para realizar operaciones bancarias incluye al menos un dispositivo de personalización 20, dispositivos para realizar operaciones bancarias 10a, 10b, dispositivos de captación de datos biométricos 40 del titular del dispositivo para realizar operaciones bancarias 10, terminales de pago 30 y/o terminales de retirada de efectivo o de realización de operaciones bancarias no mostrados en la Fig. 1.

Por ejemplo, el dispositivo de personalización 20 se incluye, de acuerdo con una primera forma de realización de la presente invención, en una institución bancaria o en una institución proveedora de dispositivos para realizar operaciones bancarias 10.

De acuerdo con una segunda forma de realización de la presente invención, el dispositivo de personalización 20 se coloca, por ejemplo, en la ventanilla de las sucursales bancarias de una institución bancaria.

Los dispositivos de captura de datos biométricos 40a y 40b se colocan, por ejemplo, de acuerdo con la presente invención, en la ventanilla de las sucursales bancarias para el dispositivo de captura de datos biométricos 40a o, por ejemplo, en un punto de venta para el dispositivo de captura de datos biométricos 40b.

De acuerdo con la presente invención, el dispositivo para realizar operaciones bancarias 10 incluye:

- medios de activación de varias órdenes a partir de identificadores de una norma relativa a las transacciones bancarias disponibles para la realización de órdenes no predefinidas por la norma,

- medios de creación, a partir de un identificador de la norma relativa a las transacciones bancarias disponible para la realización de órdenes no predefinidas por la norma, en el dispositivo para realizar operaciones bancarias, de un contenedor capaz de almacenar los datos biométricos de referencia de un usuario del dispositivo para realizar operaciones bancarias,

- medios de memorización de los datos biométricos de referencia, a partir de un identificador de la norma relativa a las transacciones bancarias disponible para la realización de órdenes no predefinidas por la norma, en el contenedor de datos biométricos de referencia del usuario del dispositivo para realizar operaciones bancarias.

La Fig. 2 muestra un ejemplo de arquitectura de un dispositivo para realizar operaciones bancarias de acuerdo con la presente invención.

El dispositivo para realizar operaciones bancarias 10 comprende:

- un procesador, microprocesador o microcontrolador 200;

- una memoria volátil 203;

- una memoria no volátil 202;

- una interfaz 205;

- un bus de comunicación que conecta el procesador 200 con la memoria ROM 203, con la memoria RAM 203 y con la interfaz 205.

El procesador 200 es capaz de ejecutar instrucciones cargadas en la memoria volátil 203 desde la memoria no volátil 202. Cuando el dispositivo para realizar operaciones bancarias 10 está encendido, el procesador 200 es capaz de leer instrucciones de la memoria volátil 203 y ejecutarlas. Estas instrucciones constituyen un programa de ordenador que hace que el procesador 200 implemente la totalidad o parte del método descrito en relación con la Fig. 8.

La totalidad o parte del método descrito en relación con la Fig. 8 se puede implementar en forma de software mediante la ejecución de un conjunto de instrucciones por parte de una máquina programable, tal como un DSP (Digital Signal Processor en inglés o Unité de Traitement de Signal Numérique en frances) o un microcontrolador, o se puede implementar en forma de hardware mediante una máquina o un componente dedicado, tal como una FPGA (matriz de puertas programables en campo) o un ASIC (circuito integrado de aplicación específica).

La interfaz 205 está adaptada para comunicarse con un dispositivo de personalización 20 y/o un terminal de pago 30.

La Fig. 3 muestra un ejemplo de arquitectura de un dispositivo para la configuración de un dispositivo para realizar operaciones bancarias de acuerdo con la presente invención.

El dispositivo de configuración 20 de un dispositivo para realizar operaciones bancarias comprende:

- un procesador, microprocesador o microcontrolador 300;

- una memoria volátil 303;

- una memoria no volátil 302;

- una interfaz 305;

- un bus de comunicación que conecta el procesador 300 con la memoria ROM 303, con la memoria RAM 303 y con la interfaz 305.

El procesador 300 es capaz de ejecutar instrucciones cargadas en la memoria volátil 303 desde la memoria no volátil 302. Cuando el dispositivo de configuración 20 está encendido, el procesador 300 es capaz de leer instrucciones de la memoria volátil 303 y ejecutarlas. Estas instrucciones constituyen un programa de ordenador que hace que el procesador 300 implemente la totalidad o parte del método descrito en relación con las Figs. 5, 6 y 7.

La totalidad o parte del método descrito en relación con las Figs. 5, 6 y 7 se puede implementar en forma de software mediante la ejecución de un conjunto de instrucciones por parte de una máquina programable, tal como un DSP (Digital Signal Processor en inglés ou Unité de Traitement de Signal Numérique en francés) o un microcontrolador, o se puede implementar en forma de hardware mediante una máquina o componente dedicado, tal como una FPGA (matriz de puertas programables en campo) o un ASIC (circuito integrado de aplicación específica).

La interfaz 305 está adaptada para comunicarse con un dispositivo para realizar operaciones bancarias 10.

La Fig. 4 muestra un ejemplo de módulos de software implementados en el dispositivo para realizar operaciones bancarias de acuerdo con la presente invención.

El dispositivo para realizar operaciones bancarias 10 incluye un módulo de activación de la función biométrica 400 que, de acuerdo con la presente invención, se utiliza para autorizar o rechazar una transacción bancaria.

Durante la creación de la aplicación para la autentificación del portador, como mínimo, mediante la verificación de los datos biométricos, el módulo de activación de la función biométrica 400 establece un parámetro específico al valor "1" lo que permite activar toda la solución implementada por la presente invención. Si este parámetro se pone a cero, el dispositivo para realizar operaciones bancarias se comporta estrictamente como un dispositivo para realizar operaciones bancarias convencionales con una autentificación por código.

Cuando el parámetro se pone a "1", entonces la funcionalidad de autentificación de datos biométricos se habilita y entonces es posible configurar la aplicación de autentificación del portador mediante la verificación de los datos biométricos, como mínimo.

El dispositivo para realizar operaciones bancarias 10 incluye un módulo de aplicación bancaria 401. El módulo de aplicación bancaria 401 se crea dentro del dispositivo para realizar operaciones bancarias con una configuración determinada que permite utilizar el código ejecutable correspondiente.

El dispositivo para realizar operaciones bancarias 10 incluye un módulo 402 que permite la interpretación de órdenes de creación de un contenedor o zona de memoria para el almacenamiento de los datos biométricos de referencia utilizados para la autentificación del portador del usuario del dispositivo para realizar operaciones bancarias 10.

Los identificadores de datos se utilizan convencionalmente en la técnica anterior durante las fases de creación de la funcionalidad de transacciones bancarias del dispositivo para realizar operaciones bancarias. De forma convencional, se envía al dispositivo para realizar operaciones bancarias 10 un identificador con los datos que identifica. Este identificador está normalizado.

De forma convencional, determinados identificadores o rangos de identificadores se reservan por las normas con el fin de identificar todos los datos cuya creación sea necesaria para el buen funcionamiento de la aplicación 401. Estas mismas normas especifican un rango de identificadores disponibles y la presente invención utiliza estos identificadores dejados disponibles, es decir, no asociados a una orden predeterminada, para especificar el tipo de orden, así como los datos a los que se refieren las órdenes.

Los identificadores utilizados por la presente invención para implementar la funcionalidad de autentificación de datos biométricos son los identificadores de la norma, tal como por ejemplo la norma EMV, llamados identificadores DGI, relacionados con las transacciones bancarias disponible para la realización de órdenes no predefinidas por la norma.

El contenedor se crea, por ejemplo, a partir de estos identificadores.

El dispositivo para realizar operaciones bancarias 10 incluye un módulo 403 que permite la interpretación de las órdenes de creación de la aplicación bancaria. Este módulo permite crear la estructura de árbol de la aplicación bancaria, es decir, los datos que la aplicación utilizará durante su funcionamiento. Estos datos son, por ejemplo, datos internos, datos de control, claves criptográficas, un código, un contador de errores de entrada de un código y un valor límite asociado.

El dispositivo para realizar operaciones bancarias 10 incluye un módulo 404 que incluye las distintas órdenes que se pueden implementar en el dispositivo para realizar operaciones bancarias 10. La lista de órdenes que se pueden implementar en el dispositivo para realizar operaciones bancarias 10 incluye, por ejemplo y sin limitación, las siguientes órdenes: registro de los datos biométricos después del suministro del dispositivo para realizar operaciones bancarias a su usuario, verificación de los datos biométricos sin encriptación, verificación de los datos biométricos con encriptación, desbloqueo del contador de errores, lectura del contador de errores.

El dispositivo para realizar operaciones bancarias 10 incluye un módulo 405 que incluye datos internos que autorizan al dispositivo para realizar operaciones bancarias 10 a realizar operaciones, tales como las descritas con referencia al módulo 404, a través de la interfaz 205 con o sin contacto físico con un terminal de pago 30.

El dispositivo para realizar operaciones bancarias 10 incluye un módulo 406 capaz de gestionar las diferentes claves criptográficas utilizadas para comunicarse por medio de la interfaz 205.

El dispositivo para realizar operaciones bancarias 10 incluye un módulo 407 que memoriza el código de autentificación, así como los diferentes contadores asociados.

El dispositivo para realizar operaciones bancarias 10 incluye un módulo 408 que gestiona la memorización de los datos biométricos en un contenedor biométrico creado.

La Fig. 5 muestra un ejemplo de un algoritmo ejecutado por un dispositivo de configuración de un dispositivo para realizar operaciones bancarias de acuerdo con una primera forma de realización de la presente invención.

El presente algoritmo se describe en un ejemplo en el que se ejecuta por el procesador 300 del dispositivo de configuración de un dispositivo para realizar operaciones bancarias.

En la etapa E500, el procesador 300 activa el módulo de activación de la función biométrica 400 utilizado para autorizar o rechazar una transacción bancaria.

El procesador 300 pone el parámetro específico en "1" y, permite de este modo activar toda la solución implementada por la presente invención y permite la activación del módulo 501.

En este caso, cabe señalar que, en una forma de realización particular de la presente invención, la etapa E500 no se realiza, siendo la activación del módulo 501 automática.

En la etapa E501, el procesador 300 activa el módulo de aplicación bancaria 401, así como el módulo 402. El módulo de aplicación bancaria 401 se crea dentro del dispositivo para realizar operaciones bancarias con una configuración determinada que permite utilizar el código ejecutable correspondiente.

En la etapa E502, el procesador 300 activa el módulo 403 que permite la creación de un contenedor para el almacenamiento de los datos biométricos de referencia utilizados para la autentificación del portador del dispositivo para realizar operaciones bancarias 10.

En la siguiente etapa E503, el procesador 300 obtiene de una base de datos biométricos, o directamente de un dispositivo de captura biométrica 40a, los datos biométricos del futuro titular o usuario del dispositivo para realizar operaciones bancarias 10. Por ejemplo, los datos biométricos han sido comunicados por el titular por medio de una red de telecomunicaciones o por medio de una sucursal bancaria de la institución bancaria.

En la etapa E504, el procesador 300 controla la memorización de los datos biométricos del futuro titular del dispositivo para realizar operaciones bancarias 10 en el contenedor creado en la etapa E502.

Las etapas E503 y E504 constituyen una operación comúnmente denominada inscripción.

En la etapa E505, el procesador 300 activa el módulo 404 que incluye las distintas órdenes que se pueden implementar en el dispositivo para realizar operaciones bancarias 10. El procesador 300 activa o no las siguientes diferentes órdenes: verificación de los datos biométricos sin encriptación, verificación de los datos biométricos con encriptación, desbloqueo del contador de errores, lectura del contador de errores.

En una forma de realización particular de la presente invención, también se activa la orden de registro de datos biométricos después del suministro del dispositivo para realizar operaciones bancarias a su titular.

En la etapa E506, el procesador 300 activa el módulo 403 que permite la interpretación de órdenes de creación de la aplicación bancaria. Este módulo permite crear la estructura de árbol de la aplicación bancaria, es decir, los datos que la aplicación utilizará durante su funcionamiento. Estos datos son, por ejemplo, datos internos, claves criptográficas, un código, un contador de errores de entrada de código y un valor límite asociado. En la misma etapa, el procesador 300 activa el módulo 405 que incluye los datos internos que autorizan al dispositivo para realizar operaciones bancarias 10 a realizar operaciones a través de la interfaz 205 con o sin contacto físico con un terminal de pago 30.

En la etapa E507, el procesador 300 activa el módulo 406 que es capaz de gestionar las diferentes claves criptográficas utilizadas para comunicarse por medio de la interfaz 205.

En la etapa E508, el procesador 300 activa el módulo 407 que memoriza el código de autentificación, así como los diferentes contadores asociados.

Una vez realizadas estas operaciones, el dispositivo para realizar operaciones bancarias 10 está listo para ser enviado a su futuro titular para su utilización inmediata.

La Fig. 6 muestra un ejemplo de un algoritmo ejecutado por un dispositivo de configuración de un dispositivo para realizar operaciones bancarias de acuerdo con una segunda forma de realización de la presente invención.

El presente algoritmo se describe en un ejemplo en el que se ejecuta por el procesador 300 del dispositivo de configuración de un dispositivo para realizar operaciones bancarias.

En la etapa E600, el procesador 300 activa el módulo de activación de la función biométrica 400 utilizado para autorizar o rechazar una transacción bancaria.

El procesador 300 pone el parámetro específico en "1" y, permite de este modo activar toda la solución implementada por la presente invención y permite la activación del módulo 501.

En este caso, cabe señalar que, en una forma de realización particular de la presente invención, la etapa E500 no se realiza, siendo la activación del módulo 501 automática.

En la etapa E601, el procesador 300 activa el módulo de aplicación bancaria 401, así como el módulo 402. El módulo de aplicación bancaria 401 se crea dentro del dispositivo para realizar operaciones bancarias con una configuración determinada que permite utilizar el código ejecutable correspondiente.

En la etapa E602, el procesador 300 activa el módulo 403 que permite la creación de un contenedor para el almacenamiento de los datos biométricos de referencia utilizados para la autentificación del portador del dispositivo para realizar operaciones bancarias 10.

En la etapa E603, el procesador 300 activa el módulo 404 que incluye las distintas órdenes que se pueden implementar en el dispositivo para realizar operaciones bancarias 10. El procesador 300, basándose en los datos internos de control, activa o no las siguientes diferentes órdenes: registro de los datos biométricos después del suministro del dispositivo para realizar operaciones bancarias a su titular, verificación de los datos biométricos sin encriptación, verificación de los datos biométricos con encriptación, desbloqueo del contador de errores, lectura del contador de errores.

En la etapa E604, el procesador 300 activa el módulo 403 que permite la interpretación de órdenes de creación de la aplicación bancaria. Este módulo permite crear la estructura de árbol de la aplicación bancaria, es decir, los datos que la aplicación utilizará durante su funcionamiento. Estos datos son, por ejemplo, datos internos, claves criptográficas, un código, un contador de errores de entrada de código y un valor límite asociado. En la misma etapa, el procesador 300 activa el módulo 405 que incluye los datos internos que autorizan al dispositivo para realizar operaciones bancarias 10 a realizar operaciones a través de la interfaz 205 con o sin contacto físico con un terminal de pago 30.

En la etapa E605, el procesador 300 activa el módulo 406 que es capaz de gestionar las diferentes claves criptográficas utilizadas para comunicarse por medio de la interfaz 205.

En la etapa E606, el procesador 300 activa el módulo 407 que memoriza el código de autentificación, así como los diferentes contadores asociados.

Una vez realizadas estas operaciones, el dispositivo para realizar operaciones bancarias 10 está listo para ser enviado al futuro titular del mismo. El titular, si quiere utilizar el dispositivo para realizar operaciones bancarias, debe acudir a una sucursal bancaria con el fin de poder proceder a una recopilación de sus datos biométricos o proporcionar sus datos biométricos con el fin de que éstos se puedan memorizar en el dispositivo para realizar operaciones bancarias 10.

La Fig. 7a muestra un ejemplo de un algoritmo ejecutado por un dispositivo de configuración de un dispositivo para realizar operaciones bancarias de acuerdo con la segunda forma de realización de la presente invención.

El presente algoritmo se describe en un ejemplo en el que se ejecuta por el procesador 300 del dispositivo de configuración de un dispositivo para realizar operaciones bancarias situado en una sucursal bancaria.

En la siguiente etapa E700, el procesador 300 obtiene los datos biométricos del futuro titular del dispositivo para realizar operaciones bancarias 10 por medio de un dispositivo de captura de datos biométricos, por ejemplo, durante la personalización de la tarjeta.

En la etapa E701, el procesador 300 controla la memorización de los datos biométricos del futuro titular del dispositivo para realizar operaciones bancarias 10 en el contenedor creado en la etapa E602 del algoritmo de Fig. 6.

Las etapas E700 y E701 constituyen una operación comúnmente denominada inscripción.

La Fig. 7b muestra un ejemplo de un algoritmo ejecutado por un dispositivo de configuración de un dispositivo para realizar operaciones bancarias de acuerdo con la presente invención.

El presente algoritmo se describe en un ejemplo en el que se ejecuta por el procesador 300 del dispositivo de configuración de un dispositivo para realizar operaciones bancarias.

En la etapa E750, el procesador 300 controla la lectura de los contadores representativos de los diferentes rechazos de transacciones bancarias relacionadas con una mala comparación entre los datos biométricos de referencia almacenados en el dispositivo para realizar operaciones bancarias y los datos candidatos.

Si los contadores tienen un valor inferior a un valor máximo, el procesador 300 interrumpe el presente algoritmo.

Si los contadores tienen un valor mayor o igual al valor máximo, el procesador 300 pasa a la etapa E751.

En la etapa E751, el procesador 300 controla el desbloqueo de los contadores leidos poniendo éstos a un valor cero e interrumpe el presente algoritmo.

En una forma de realización particular, si la frecuencia de desbloqueo de los contadores es significativa, por ejemplo, una periodicidad mensual, el procesador 300 pasa de la etapa E751 al E752.

En la siguiente etapa E752, el procesador 300 obtiene datos biométricos del futuro titular del dispositivo para realizar operaciones bancarias 10 por medio de un dispositivo de captura de datos biométricos.

En la etapa E753, el procesador 300 controla la memorización de los datos biométricos obtenidos en la etapa E752 en el contenedor creado en la etapa E602 del algoritmo de la Fig. 6 en lugar de los datos biométricos previamente almacenados.

La Fig. 8 muestra un ejemplo de un algoritmo ejecutado por un dispositivo para realizar operaciones bancarias de acuerdo con la presente invención.

El presente algoritmo se describe en un ejemplo en el que es ejecutado por el procesador 200 del dispositivo para realizar operaciones bancarias 10.

En la etapa E800, el procesador 200 comprueba si el dispositivo para realizar operaciones bancarias 10 recibe una orden de un terminal de pago 30.

En caso afirmativo, el procesador 200 pasa a la etapa E801. En caso negativo, el procesador 200 pasa a la etapa E806.

En la etapa E801, el procesador 200 recibe los datos biométricos candidatos tomados por un dispositivo de captura de datos biométricos asociado al terminal de pago al que está conectado el dispositivo para realizar operaciones bancarias 10.

En la siguiente etapa E802, el procesador 200 compara los datos biométricos candidatos con los datos de referencia almacenados en el contenedor del dispositivo para realizar operaciones bancarias 10.

Si la comparación de los datos biométricos candidatos con los datos de referencia almacenados en el contenedor del dispositivo para realizar operaciones bancarias 10 es positiva, el procesador 200 pasa a la etapa E805. En caso negativo, el procesador 200 pasa a la etapa E803.

En la etapa E803, el procesador 200 rechaza la transacción bancaria.

En la siguiente etapa E804, el procesador 200 incrementa los contadores representativos de los diferentes rechazos de transacciones bancarias relacionados con una mala comparación entre los datos biométricos de referencia almacenados en el dispositivo para realizar operaciones bancarias y los datos candidatos.

Una vez realizada esta operación, el procesador 200 vuelve a la etapa E800.

Si los contadores tienen un valor mayor o igual al valor máximo, el procesador 300 bloquea la posibilidad de realizar transacciones bancarias por medio del dispositivo para realizar operaciones bancarias 10.

En una forma de realización particular de la presente invención, si los contadores tienen un valor mayor o igual al valor máximo, el procesador 300 selecciona otro modo de autentificación del usuario del dispositivo, y si es necesario, rechaza cualquier operación bancaria mientras el contador de rechazos no se haya actualizado.

En la etapa E805, el procesador 200 acepta la transacción bancaria.

Una vez realizada esta operación, el procesador 200 vuelve a la etapa E800.

En la etapa E806, el procesador 200 comprueba si se recibe una orden de lectura de los contadores representativos de los diferentes rechazos de transacciones bancarias relacionados con una mala comparación entre los datos biométricos de referencia almacenados en el dispositivo para realizar operaciones bancarias y los datos candidatos.

En caso afirmativo, el procesador 200 pasa a la etapa E806. En caso negativo, el procesador pasa a la etapa E808.

En la etapa E807, se leen los contadores representativos de los diferentes rechazos de transacciones bancarias relacionados con una mala comparación entre los datos biométricos de referencia almacenados en el dispositivo para realizar operaciones bancarias y los datos candidatos.

Una vez realizada esta operación, el procesador 200 vuelve a la etapa E800.

En la etapa E808, el procesador 200 comprueba si se recibe una orden de actualización de los contadores representativos de los diferentes rechazos de operaciones bancarias relacionados con una mala comparación entre los datos biométricos de referencia almacenados en el dispositivo para realizar operaciones bancarias y los datos candidatos.

Si se recibe una orden para actualizar los contadores representativos de los diferentes rechazos de operaciones bancarias relacionados con una mala comparación entre los datos biométricos de referencia almacenados en el dispositivo para realizar operaciones bancarias y los datos candidatos, el procesador 200 pasa a la etapa E809. En caso negativo, el procesador 200 pasa a la etapa E810.

En la etapa E809, se actualizan los contadores representativos de los diferentes rechazos de transacciones bancarias relacionados con una mala comparación entre los datos biométricos de referencia almacenados en el dispositivo para realizar operaciones bancarias y los datos candidatos.

Una vez realizada esta operación, el procesador 200 vuelve a la etapa E800.

En la etapa E810, el procesador 200 comprueba si se ha recibido una orden de actualización de los datos biométricos de referencia almacenados en el dispositivo para realizar operaciones bancarias y los datos candidatos.

Si se recibe una orden para actualizar los datos biométricos de referencia almacenados en el dispositivo para realizar operaciones bancarias y los datos candidatos, el procesador 200 pasa a la etapa E811. En caso negativo, el procesador 200 vuelve a la etapa E800.

En la etapa E811, se memorizan nuevos datos biométricos en el contenedor.

Una vez realizada esta operación, el procesador 200 vuelve a la etapa E800.

Por supuesto, la presente invención no se limita en absoluto a las formas de realización descritas en la presente memoria, sino que abarca cualquier variante al alcance del experto en la técnica.

REIVINDICACIONES

1. Método de configuración de un dispositivo para realizar operaciones bancarias en el que se utilizan los datos biométricos del titular del dispositivo para realizar operaciones bancarias para autenticar al usuario del dispositivo para realizar operaciones bancarias, caracterizado por que el método incluye las etapas, realizadas durante la configuración del dispositivo para realizar operaciones bancarias, de:

- activación o no en el dispositivo para realizar operaciones bancarias de una funcionalidad de datos biométricos para autenticar al usuario del dispositivo para realizar operaciones bancarias,

- activación de varias órdenes a partir de identificadores de una norma relativa a las transacciones bancarias disponibles para la realización de órdenes no predefinidas por la norma,

- creación (E502), a partir de un identificador de la norma relativa a las transacciones bancarias disponible para la realización de órdenes no predefinidas por la norma, en el dispositivo para realizar operaciones bancarias, de un contenedor capaz de memorizar los datos biométricos de referencia de un usuario del dispositivo para realizar operaciones bancarias,

- memorización (E504) de los datos biométricos de referencia, a partir de un identificador de la norma relativa a las transacciones bancarias disponible para la realización de órdenes no predefinidas por la norma, en el contenedor de datos biométricos de referencia del usuario del dispositivo para realizar operaciones bancarias.

2. Método de acuerdo con la reivindicación 1, caracterizado por que el método incluye además las etapas de:

- recepción de los datos biométricos candidatos para una operación bancaria,

- comparación de los datos biométricos candidatos con los datos biométricos de referencia,

- autorización o rechazo de la operación bancaria en función de la comparación.

3. Método de acuerdo con una cualquiera de las reivindicaciones 1 a 2, caracterizado por que el método incluye además la etapa de memorización en el dispositivo para realizar operaciones bancarias de instrucciones capaces de procesar al menos una de las siguientes órdenes: verificación de los datos biométricos sin encriptación, verificación de los datos biométricos con encriptación, desbloqueo de un contador de errores, lectura de un contador de errores.

4. Método de acuerdo con una cualquiera de las reivindicaciones 1 a 2, caracterizado por que el método incluye además la etapa de memorización en el dispositivo para realizar operaciones bancarias de instrucciones capaces de procesar el registro de datos biométricos con posterioridad al suministro del dispositivo para realizar operaciones bancarias a su usuario.

5. Método de acuerdo con una de las reivindicaciones precedentes, caracterizado por que, en caso de rechazo de la operación bancaria, el método incluye además la etapa del incremento de un contador de rechazos.

6. Método de acuerdo con la reivindicación 5, caracterizado por que el método incluye además las etapas de comparar el valor del contador de rechazos con un valor predeterminado y, si el valor del contador de rechazos es igual al valor predeterminado, seleccionar otro modo de autentificación del usuario del dispositivo y, si es necesario, rechazar cualquier operación bancaria mientras el contador de rechazos no se haya actualizado.

7. Método de acuerdo con la reivindicación 5, caracterizado por que cuando se actualiza el contador de rechazos, el método incluye además la etapa de actualizar en el contenedor nuevos datos biométricos de referencia del usuario del dispositivo para realizar operaciones bancarias.

8. Método de acuerdo con una cualquiera de las reivindicaciones precedentes caracterizado por que, si la funcionalidad de los datos biométricos no está activada, el método incluye las etapas de:

- recepción de un código de autentificación candidato para una operación bancaria,

- comparación del código de autentificación candidato con un código de referencia memorizado en el dispositivo para realizar operaciones bancarias,

- autorización o rechazo de la operación bancaria en función de la comparación del código de autentificación candidato con el código de referencia.

9. Dispositivo para realizar operaciones bancarias en el que se utilizan los datos biométricos del titular del dispositivo para realizar operaciones bancarias para autenticar al usuario del dispositivo para la realización de transacciones bancarias, caracterizado por que el dispositivo incluye:

- medios de activación o desactivación, en el dispositivo para realizar operaciones bancarias, de una funcionalidad de datos biométricos para autenticar al usuario del dispositivo para realizar operaciones bancarias,

- medios de activación durante la configuración del dispositivo para realizar operaciones bancarias de varias órdenes a partir de identificadores de una norma relativa a las transacciones bancarias disponibles para la realización de órdenes no predefinidas por la norma,

- medios de creación, activados durante la configuración del dispositivo para realizar operaciones bancarias, a partir de un identificador de la norma relativa a las transacciones bancarias disponible para la realización de órdenes no predefinidas por la norma, en el dispositivo para realizar operaciones bancarias, de un contenedor capaz de memorizar los datos biométricos de referencia de un usuario del dispositivo para realizar operaciones bancarias,

- medios de memorización de los datos biométricos de referencia, activados durante la configuración del dispositivo para realizar operaciones bancarias, a partir de un identificador de la norma relativa a las transacciones bancarias disponible para la realización de órdenes no predefinidas por la norma, en el contenedor de datos biométricos de referencia del usuario del dispositivo para realizar operaciones bancarias.

10. Tarjeta con chip caracterizada por que incluye el dispositivo para realizar operaciones bancarias de acuerdo con la reivindicación 9.

11. Programa informático almacenado en un soporte de informaciones, incluyendo dicho programa instrucciones que permiten implementar el método de acuerdo con una cualquiera de las reivindicaciones 1 a 8, cuando se carga y ejecuta mediante un sistema informático.

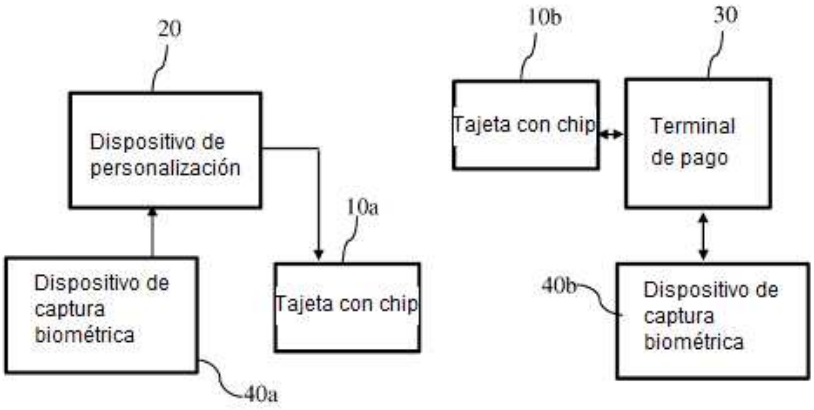
20
Dispositivo de personalización
10a
Dispositivo de captura biométrica
Tajeta con chip
40a
10b
30
Tajeta con chip
Terminal de pago
40b
Dispositivo de captura biométrica

Fig. 1

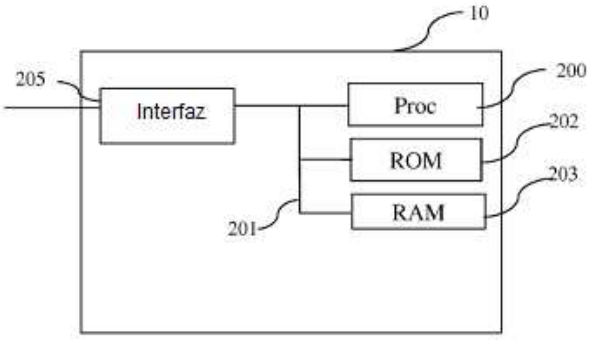
10
205
Interfaz
Proc
200
202
ROM
203
RAM
201

Fig. 2

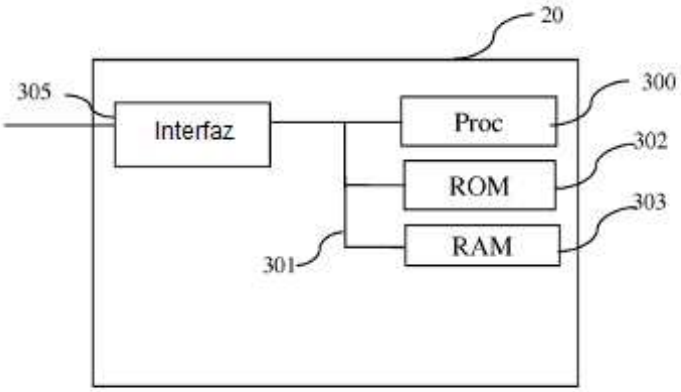
20
305
Interfaz
Proc
300
302
ROM
303
RAM
301

Fig. 3

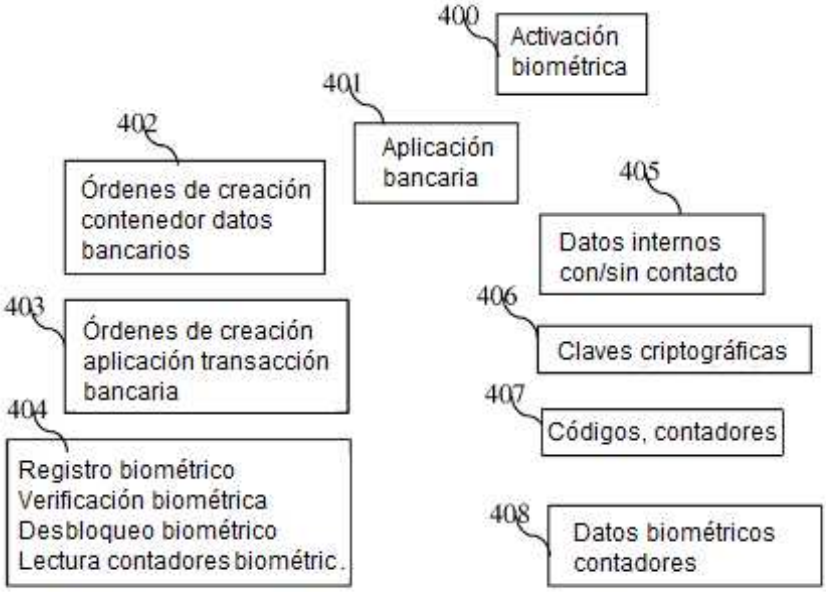
400
Activación biométrica
401
Aplicación bancaria
402
Órdenes de creación contenedor datos bancarios
405
Datos internos con/sin contacto
403
Órdenes de creación aplicación transacción bancaria
406
Claves criptográficas
404
Registro biométrico
Verificación biométrica
Desbloqueo biométrico
Lectura contadores biométric.
407
Códigos, contadores
408
Datos biométricos contadores

Fig. 4

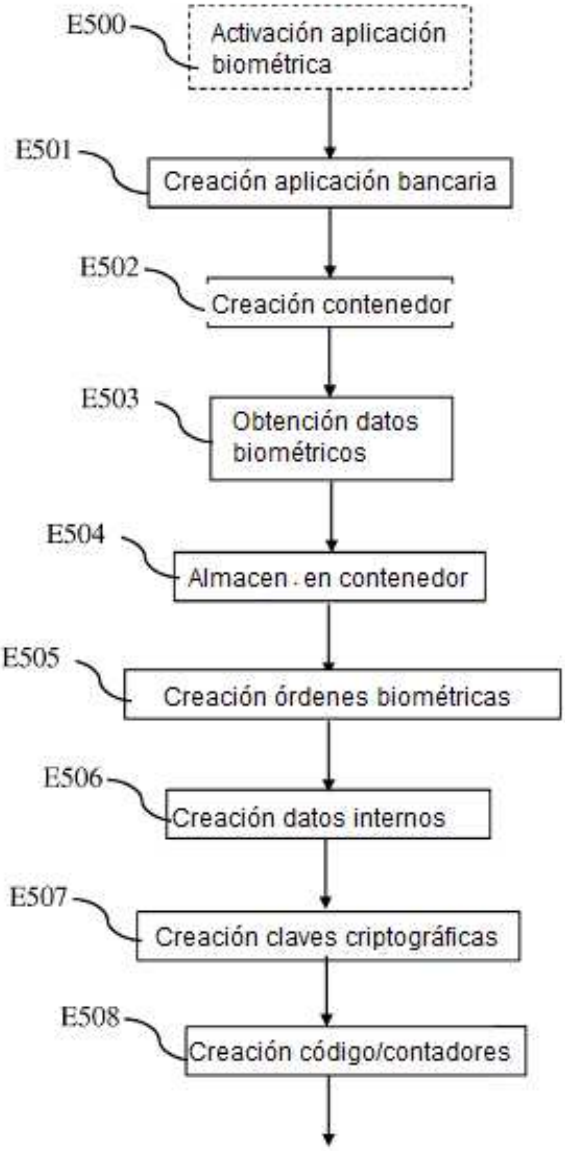
E500
Activación aplicación biométrica
E501
Creación aplicación bancaria
E502
Creación contenedor
E503
Obtención datos biométricos
E504
Almacen. en contenedor
E505
Creación órdenes biométricas
E506
Creación datos internos
E507
Creación claves criptográficas
E508
Creación código/contadores

Fig. 5

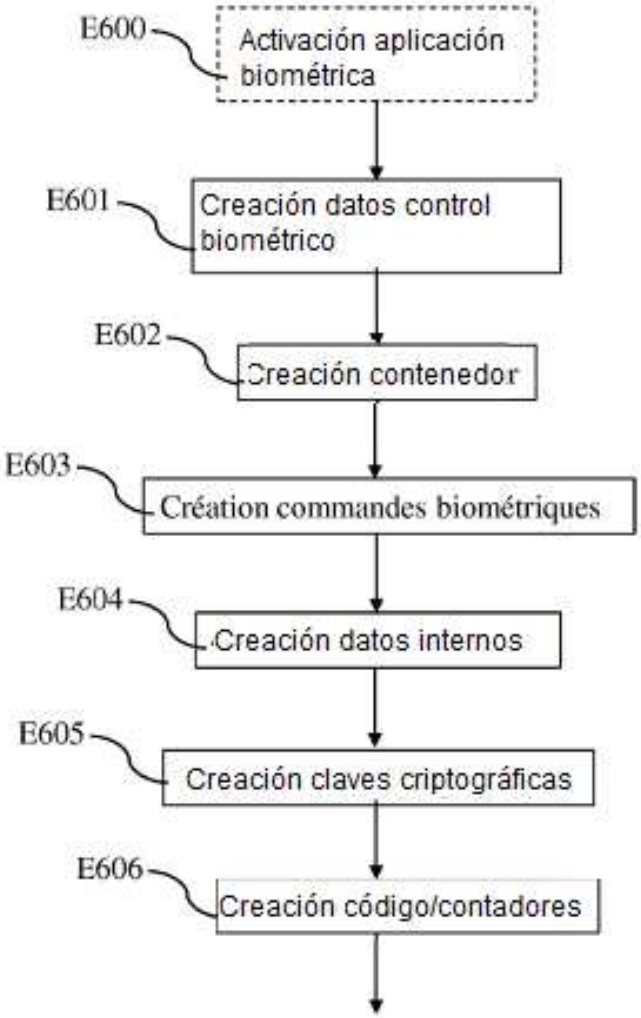
E600
Activación aplicación biométrica
E601
Creación datos control biométrico
E602
Creación contenedor
E603
Création commandes biométriques
E604
Creación datos internos
E605
Creación claves criptográficas
E606
Creación código/contadores

Fig. 6

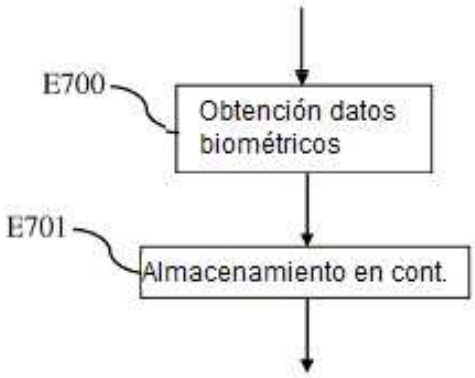
E700
Obtención datos biométricos
E701
Almacenamiento en cont.

Fig. 7a

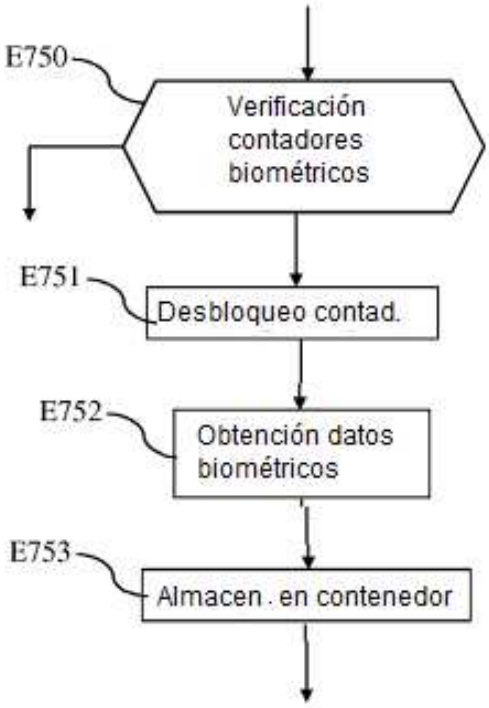
E750
Verificación contadores biométricos
E751
Desbloqueo contad.
E752
Obtención datos biométricos
E753
Almacen . en contenedor

Fig. 7b

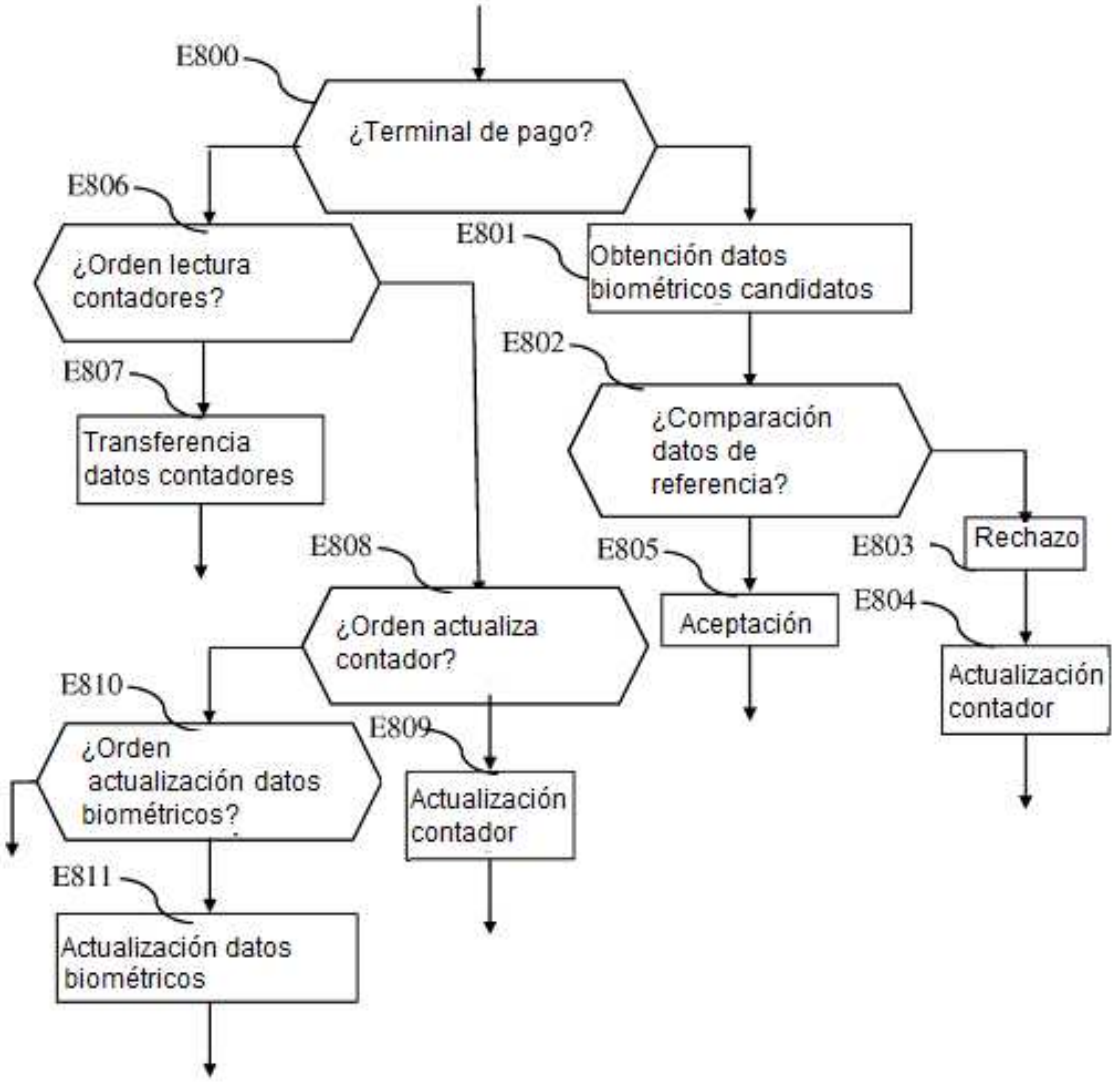
E800
¿Terminal de pago?
E806
¿Orden lectura contadores?
E801
Obtención datos biométricos candidatos
E807
Transferencia datos contadores
E802
¿Comparación datos de referencia?
E808
¿Orden actualiza contador?
E805
Aceptación
E803
Rechazo
E804
Actualización contador
E810
¿Orden actualización datos biométricos?
E809
Actualización contador
E811
Actualización datos biométricos

Fig. 8