(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 790 645**

(51) Int. CI.:

G06F 21/31 (2013.01)
G06F 21/36 (2013.01)
G06Q 20/32 (2012.01)
H04W 12/06 (2009.01)
G06Q 20/40 (2012.01)
G07F 7/08 (2006.01)
G07F 7/10 (2006.01)
G06F 21/83 (2013.01)
G09C 5/00 (2006.01)
H04L 9/32 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **01.12.2016 PCT/IB2016/057249**

(87) Fecha y número de publicación internacional: **06.07.2017 WO17115174**

(96) Fecha de presentación y número de la solicitud europea: **01.12.2016 E 16881348 (3)**

(97) Fecha y número de publicación de la concesión europea: **12.02.2020 EP 3381003**

(54) Título: **Sistema y método para autenticar a un usuario en un dispositivo**

(30) Prioridad:

28.12.2015 US 201562271428 P

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
28.10.2020

(73) Titular/es:

MOBEEWAVE INC. (100.0%)
80 rue Queen
Montreal, Québec H3C 2N5, CA

(72) Inventor/es:

OLLIVIER, JULIEN;
ALIMI, VINCENT y
FONTAINE, SÉBASTIEN

(74) Agente/Representante:

ELZABURU, S.L.P

DESCRIPCIÓN

Sistema y método para autenticar a un usuario en un dispositivo

Referencia

La presente solicitud reivindica prioridad de la convención a la Solicitud de Patente Provisional de U.S. Nº 62/271,428, presentada el 28 de diciembre de 2015, titulada “SYSTEM FOR AND METHOD OF AUTHENTICATING A USER ON DEVICE”.

Campo

La presente tecnología se refiere a sistemas y métodos para autenticar a un usuario en dispositivos móviles. El sistema y el método pueden ser utilizados en el contexto de la realización de transacciones en un dispositivo móvil, más particularmente transacciones financieras seguras.

Antecedentes

Esta sección pretende introducir al lector en diversos aspectos de a técnica que pueden estar relacionados con diversos aspectos de la presente invención, que están descritos y/o son reivindicados en lo que sigue. Esta explicación se cree que es útil para proporcionar al lector información de antecedentes para facilitar una mejor comprensión de los diversos aspectos de la presente tecnología. En consecuencia, se debe entender que estas declaraciones deben ser leídas a la luz de la misma, y no como reconocimientos de la técnica anterior.

Los terminales de pago, también conocidos como terminales de punto de venta (POS – Point of Sale, en inglés), están bien consolidados en la técnica. Se utilizan para transferencias electrónicas de fondos entre comercios y clientes, donde las transacciones se realizan deslizando, insertando o tocando tarjetas de pago con un terminal POS. Algunos terminales POS solo soportan la tecnología de banda magnética (deslizamiento), mientras que otros terminales soportan, de manera adicional o exclusiva, las llamadas tarjetas con chip o tarjetas inteligentes, que comprenden un chip de microprocesador integrado en la tarjeta. Este chip proporciona un alto nivel de seguridad contra ataques lógicos y físicos dirigidos a clonar la tarjeta o poner en peligro la información confidencial almacenada en la misma.

Con el fin de garantizar la seguridad durante las transacciones financieras que involucran tarjetas con chip, se han desarrollado y utilizado estándares de seguridad tales como el estándar de transacción Europay, MasterCard y Visa (EMV) para certificar tanto los terminales de pago como las tarjetas de pago. No obstante, debido a diversos factores, incluida la complejidad técnica requerida para cumplir con los estándares de seguridad, los terminales de pago que se utilizan para realizar transacciones financieras seguras suelen ser dispositivos engorrosos, costosos y dedicados de manera exclusiva a la realización de transacciones financieras.

Los sistemas de pago móvil y los monederos digitales, tales como Apple Pay®, Android Pay® y Samsung Pay® permiten a los clientes almacenar la información de su tarjeta de crédito en sus dispositivos móviles y utilizar sus dispositivos para realizar pagos por medio de la comunicación de campo cercano (NFC – Near Field Communication, en inglés) o la identificación por radiofrecuencia (RFID – Radio-Frequency IDentification, en inglés) en terminales adaptados de punto de venta sin contacto.

No obstante, los dispositivos móviles pueden no tener los estándares de seguridad requeridos para ser utilizados como terminales de pago, no son aceptados en todas partes y, por lo tanto, no eliminan por completo la necesidad de terminales de pago exclusivos.

Como respuesta, al menos, a algunas de las deficiencias de las tecnologías detalladas anteriormente, se han desarrollado enfoques para permitir que un dispositivo móvil de utilización general, tal como, entre otros, un teléfono inteligente, se convierta en un terminal de pago. Dichos enfoques incluyen el método, dispositivo, complemento y elemento seguro de la publicación de patente de U.S. Nº 2014/0324698, en donde se proporcionan un método y un dispositivo para realizar una transacción financiera segura, comprendiendo el dispositivo una CPU y un elemento seguro, en donde se obtiene el importe de una compra para ser cargado en una cuenta financiera, se obtienen los datos relativos a la cuenta financiera y se obtiene una autorización de transacción de una institución financiera relacionada con la transacción financiera, estando basada la autorización, al menos parcialmente, en datos procesados únicamente por el elemento seguro, con independencia de los datos procesado por la CPU.

Además, se han desarrollado métodos y sistemas para abordar la necesidad de autenticar de manera segura a un usuario, por medio de su número de identificación personal (PIN – Personal Identification Number, en inglés), cuando realiza una transacción financiera utilizando una tarjeta de pago en un terminal de punto de venta exclusivo. Dichos métodos y sistemas, mediante los cuales el terminal de pago actúa como un dispositivo de entrada de PIN (PED – Pin Entry Device, en inglés), están dirigidos a cumplir con el nivel de seguridad requerido especificado en estándares internacionales tales como ISO 9564, industria de las tarjetas de pago (PCI – Payment Card Industry, en inglés) - Seguridad de transacción mediante PIN (PTS – PIN Transaction Security, en inglés), y otros estándares de PCI aplicables, que han sido desarrollados para la seguridad y la gestión mediante PIN en la banca para comercios, comprendiendo los estándares requisitos para la longitud del PIN, selección, emisión, entrega, algoritmos de

encriptado, almacenamiento, transmisión, entrada segura y requisitos para el manejo de PIN fuera de línea en cajeros automáticos y sistemas POS.

El documento US 2013/301830 A1 da a conocer un sistema y un método de entrada segura, para el manejo de contraseñas y números de identificación personal (PIN) para pagos seguros a través de dispositivos móviles.

El documento US 2015/154414 A1 da a conocer un método de autenticación implementado por ordenador, que comprende la etapa de permitir que un usuario introduzca un identificador (por ejemplo, un PIN) en un dispositivo electrónico que tiene una pantalla y un teclado accionables dentro de una zona de teclado de la pantalla.

El documento EP 2 775 421 A1 da a conocer un terminal de punto de venta (POS) para introducir un PIN para permitir una transacción financiera, que comprende una pantalla táctil para mostrar información y recibir entradas del usuario.

Andrea Forte et al.: “EyeDecrypt – Private Interactions in Plain Sight”, International Association for Cryptologic Research, vol. 20140625: 194801, 25 de junio de 2014, da a conocer una tecnología para la interacción entre una persona y un ordenador, que mantiene la privacidad.

Otros enfoques se centran, en general, en terminales de pago voluminosos, donde el dispositivo recibe una imagen aleatorizada mediante el PIN, es superpuesta en la parte superior de un teclado subyacente, de modo que un usuario introduce una versión codificada de su PIN, y la versión codificada es enviada a continuación, preferiblemente, a un servidor remoto, y es descodificada para procesar el PIN. No obstante, tales métodos pueden no cumplir completamente con los estándares de seguridad financiera, pueden no permitir el procesamiento fuera de línea y/o pueden no estar habilitados en un dispositivo móvil para ser utilizado como terminal de pago.

Por lo tanto, existe la necesidad en la técnica de un método y un sistema para obtener un código de identificación personal (PIC – Personal Identification Code, en inglés) en un dispositivo móvil a la vez que se proporciona un cierto nivel de seguridad, minimizando el coste adicional y/o la interrupción del diseño (por ejemplo, limitando y/o eliminando la necesidad de componentes de hardware que no están presentes en el dispositivo por otras razones). Dicho nivel de seguridad puede ser seleccionado, pero no necesariamente, para cumplir con ciertos estándares de seguridad.

Compendio

Las realizaciones de la presente tecnología han sido desarrolladas en base a la apreciación de los inventores de que los enfoques conocidos para la introducción segura del PIN pueden, en algunos casos, no ser fiables para realizar transacciones financieras seguras que cumplan con los estándares de la industria financiera en dispositivos móviles. Por lo tanto, son deseables mejoras, en particular mejoras destinadas a garantizar que un PIC sea almacenado en un entorno seguro, o en forma encriptada en un entorno no seguro, y mejoras destinadas a reducir los riesgos de intercepción del PIC por un software malicioso.

La presente tecnología surge de una observación realizada por el inventor o los inventores de que, si bien la utilización de dispositivos móviles se ha democratizado, la mayoría de las transacciones financieras todavía se realizan utilizando terminales de pago voluminosos, debido a la falta de métodos seguros para realizar la introducción del PIC en un dispositivo móvil. No obstante, a la luz de los últimos desarrollos en la técnica, el inventor o los inventores han ideado un método y un sistema para realizar transacciones financieras seguras en un dispositivo móvil a la vez que proporcionan un cierto nivel de seguridad.

El objeto de la presente tecnología es resuelto mediante un método para accionar un dispositivo, de acuerdo con la reivindicación 1, y un sistema implementado por ordenador, de acuerdo con la reivindicación 12. Las realizaciones preferidas se presentan en las reivindicaciones dependientes.

En general, otro aspecto del tema descrito en la memoria descriptiva puede estar realizado en un método y un sistema que comprende, además, antes de transmitir, al elemento seguro, la tabla de correspondencia, encriptar la tabla de correspondencia.

En general, otro aspecto del tema descrito en la memoria descriptiva puede estar realizado en un método y un sistema que comprende, además, después de encriptar la tabla de correspondencia, desencriptar, mediante el elemento seguro, la tabla de correspondencia.

En general, otro aspecto del tema descrito en la memoria descriptiva puede estar realizado en un método y un sistema en donde una versión sin encriptar del PIC permanece inaccesible para cualquiera del procesador, el controlador de la pantalla, el controlador de la pantalla táctil y el área segura aislada del procesador, en cualquier momento.

En general, otro aspecto del tema descrito en la memoria descriptiva puede estar realizado en un método y un sistema en donde una versión sin encriptar del PIC es accesible únicamente por el elemento seguro.

En general, otro aspecto del tema descrito en la memoria descriptiva puede estar realizado en un método y un sistema en donde el área segura aislada solo accede a una versión encriptada del PIC.

En general, otro aspecto del tema descrito en la memoria descriptiva puede estar realizado en un método y un sistema en donde el controlador de la pantalla táctil no tiene acceso a la tabla de correspondencia ni a la representación visual del teclado aleatorizado, en cualquier momento.

En general, otro aspecto del tema descrito en la memoria descriptiva puede estar realizado en un método y un sistema en donde el elemento seguro está conectado de manera segura al procesador.

En general, otro aspecto del tema descrito en la memoria descriptiva puede estar realizado en un método y un sistema en el que el área segura aislada del procesador comprende una interfaz de usuario fiable.

En general, otro aspecto del tema descrito en la memoria descriptiva puede estar realizado en un método y un sistema en donde el controlador de la pantalla táctil está conectado de manera segura a la interfaz de usuario fiable.

En general, otro aspecto del tema descrito en la memoria descriptiva puede estar realizado en un método y un sistema en donde el método comprende, además volver a aleatorizar, al menos, una parte de la representación visual del teclado aleatorizado, mediante la generación de una tabla de correspondencia después de que ocurra un evento de codificación.

En general, otro aspecto del tema descrito en la memoria descriptiva puede estar realizado en un método y un sistema en donde se generan múltiples tablas de correspondencia, disposiciones de puntos de conexión y representaciones visuales de teclados codificados antes de que ocurra un evento táctil.

En general, otro aspecto del tema descrito en la memoria descriptiva puede estar realizado en un método y un sistema en donde la representación visual del teclado aleatorizado es, al menos una, de una imagen, una secuencia de video y una representación visual de un teclado.

En general, otro aspecto del tema descrito en la memoria descriptiva puede estar realizado en un método y un sistema en donde el método comprende, además, hacer que el controlador de la pantalla muestre un indicador de seguridad previamente asociado con el usuario.

En general, otro aspecto del tema descrito en la memoria descriptiva puede estar realizado en un método y un sistema en donde el indicador de seguridad previamente asociado con el usuario está almacenado en el área segura aislada del procesador.

En general, otro aspecto del tema descrito en la memoria descriptiva puede estar realizado en un método y un sistema que comprende, además, encriptar el PIC reconstituido por el elemento seguro; y transmitir el PIC reconstituido encriptado al procesador.

En general, otro aspecto del tema descrito en la memoria descriptiva puede estar realizado en un método y un sistema en donde el elemento seguro es, al menos, uno de un elemento de hardware conectado operativamente al procesador, un componente de software ejecutado por el procesador, el área segura aislado y una porción del área segura aislada.

En general, otro aspecto del tema descrito en la memoria descriptiva puede estar realizado en un método y un sistema en donde la generación de la tabla de correspondencia, el diseño de puntos de conexión y la representación visual del teclado aleatorizado son ejecutados en uno del área segura aislada del procesador y el elemento seguro.

En general, otro aspecto del tema descrito en la memoria descriptiva puede estar realizado en un método y un sistema en donde la reconstitución del PIC asociado con el usuario comprende asignar los eventos de codificación en la tabla de correspondencia.

En general, otro aspecto del tema descrito en la memoria descriptiva puede estar realizado en un método y un sistema en un dispositivo móvil para realizar transacciones financieras seguras entre, al menos, dos dispositivos móviles (“banca de igual a igual”)

En otros aspectos, diversas implementaciones de la presente tecnología proporcionan un medio no transitorio, legible por ordenador, que almacena instrucciones informáticas para realizar la introducción del PIC segura en un dispositivo, siendo ejecutables las instrucciones informáticas por un procesador de un sistema informático para llevar a cabo uno o más de los métodos mencionados anteriormente.

En otros aspectos, diversas implementaciones de la presente tecnología proporcionan un sistema basado en un ordenador, tal como, por ejemplo, pero sin ser limitativo, un dispositivo que comprende, al menos, un procesador e instrucciones informáticas de almacenamiento de memoria para realizar una introducción del PIC segura en un dispositivo, siendo ejecutables las instrucciones informáticas por uno o más procesadores del sistema informático para llevar a cabo uno o más de los métodos mencionados anteriormente.

Los detalles de una o más realizaciones del tema de esta memoria descriptiva se exponen en los dibujos adjuntos y en la descripción que sigue. Otras características, aspectos y ventajas del tema serán evidentes a partir de la descripción, los dibujos y las reivindicaciones.

Breve descripción de los dibujos

Estas y otras características, aspectos y ventajas de la presente tecnología se comprenderán mejor con respecto a la siguiente descripción, reivindicaciones adjuntas y dibujos adjuntos, donde:

la figura 1 es una ilustración de los componentes y características del dispositivo, de acuerdo con una realización de la presente tecnología;

la figura 2a es una ilustración de una posible tabla de correspondencia, de acuerdo con una realización de la presente tecnología;

la figura 2b es una ilustración de un posible diseño de puntos de conexión, de acuerdo con una realización de la presente tecnología;

la figura 2c es una ilustración de una posible disposición de un teclado aleatorizado, de acuerdo con una realización de la presente tecnología;

la figura 3 es una ilustración de una posible pantalla de autenticación de código de identificación personal (PIC), de acuerdo con una realización de la presente tecnología;

la figura 4 es una representación de diagrama de flujo de un flujo de comunicación entre un procesador, un controlador de pantalla, un controlador de pantalla táctil y un elemento seguro, de acuerdo con una realización de la presente tecnología; y

la figura 5 es una ilustración de un método llevado a cabo de acuerdo con las realizaciones no limitativas de la presente tecnología.

Descripción detallada de los dibujos

A continuación, se describirán diversas realizaciones a modo de ejemplo de la tecnología descrita más detalladamente con referencia a los dibujos adjuntos, en los que se muestran realizaciones a modo de ejemplo. No obstante, el presente concepto inventivo puede ser realizado de muchas formas diferentes, y no debe ser interpretado como limitado a las realizaciones a modo de ejemplo expuestas en el presente documento. Más bien, estas realizaciones a modo de ejemplo se proporcionan de modo que la invención sea exhaustiva y completa, y transmita completamente el alcance del presente concepto inventivo a los expertos en la materia. En los dibujos, los tamaños y los tamaños relativos de capas y regiones pueden estar exagerados por razones de claridad. Números iguales se refieren a elementos iguales en todo el documento.

Se comprenderá que, aunque los términos primero, segundo, tercero, etc. pueden ser utilizados en el presente documento para describir diversos elementos, estos elementos no deben estar limitados por estos términos. Estos términos se utilizan para distinguir un elemento de otro. Por lo tanto, un primer elemento explicado a continuación podría denominarse un segundo elemento sin apartarse de las explicaciones del presente concepto inventivo. Tal como se utiliza en el presente documento, el término “y/o” incluye cualquiera y todas las combinaciones de uno o más de los elementos enumerados asociados.

Se comprenderá que, cuando se hace referencia a un elemento como “conectado” o “acoplado” a otro elemento, puede estar directamente conectado o acoplado al otro elemento o pueden estar presentes elementos intermedios. Por el contrario, cuando se hace referencia a un elemento como “conectado directamente” o “acoplado directamente” a otro elemento, no hay ningún elemento intermedio presente. Otras expresiones utilizadas para describir la relación entre elementos deben ser interpretadas de manera similar (por ejemplo, “entre” frente a “directamente entre”, “adyacente” frente a “directamente adyacente”, etc.)

La terminología utilizada en el presente documento solo pretende describir realizaciones particulares a modo de ejemplo, y no pretende limitar el presente concepto inventivo. Tal como se utiliza en el presente documento, las formas singulares “un”, “una”, “el” y “la” pretenden incluir también las formas plurales, a menos que el contexto indique claramente lo contrario. Se comprenderá, además, que los términos “comprende” y/o “que comprende”, cuando se utilizan en esta memoria descriptiva, especifican la presencia de características, números enteros, etapas, operaciones, elementos y/o componentes establecidos, pero no excluyen la presencia o adición de una o más características, números enteros, etapas, operaciones, elementos, componentes y/o grupos de los mismos.

A lo largo de la presente invención, se hace referencia a transacciones seguras (por ejemplo, pero sin ser limitativo, transacciones con contacto y sin contacto), elementos seguros (por ejemplo, pero sin ser limitativo, chipset, chipset seguro, componente seguro de incrustación de hardware, componente seguro de incrustación de software o componente seguro de incrustación de firmware) y estándares de seguridad. Ejemplos de estándares de seguridad incluyen, sin ser limitativos, estándares de certificación de Europay, MasterCard y Visa (EMV), EMVCo, MasterCard®, Visa®, American Express®, JCB®, Discover® y de SSC de PCI (Payment Card Industry Security Standards Council), fundado por MasterCard®, Visa®, American Express®, Discover® y JCB® y que se ocupa, específicamente, de la definición de estándares de seguridad para transacciones financieras. La referencia a transacciones seguras,

elementos seguros y normas de seguridad se hace con fines ilustrativos y pretende ser un ejemplo de la presente tecnología, y no limitar el alcance de la misma.

Procesador: en el contexto de esta tecnología, la definición de procesador incluye un sistema en chip (SoC – System on Chip, en inglés), un circuito integrado que integra los componentes de un ordenador en un solo chip. Un SoC típico puede incluir, entre otros, uno o más microprocesadores de uso general o unidades de procesamiento central (CPU – Central Processing Units, en inglés), coprocesadores tales como un procesador de señal digital (DSP – Digital Processing System, en inglés), una unidad de procesamiento de gráficos (GPU – Graphics Processing Unit, en inglés) y procesadores multimedia, tales como codificadores y descodificadores MPEG y JPEG. El SoC puede incluir, asimismo, módems para diversas interfaces de comunicaciones inalámbricas que incluyen celular (por ejemplo, LTE / 4G, 3G, GSM, CDMA, etc.), Bluetooth y fidelidad inalámbrica (Wi-Fi – Wireless Fidelity, en inglés) (IEEE 802.11). El SoC puede incluir controladores de memoria para interactuar con chips de memoria DRAM externos o internos, y bloques de memoria internos que incluyen una selección de ROM, SRAM, DRAM, EEPROM y memoria flash. El SoC puede incluir, adicionalmente, fuentes de temporización, periféricos, que incluyen contadores de tiempo, temporizadores en tiempo real y generadores de reinicio de encendido, depuración, JTAG e interfaces de diseño para prueba (DFT – Design For Test, en inglés), interfaces externas, interfaces analógicas, reguladores de tensión, circuitos de gestión de la potencia, etc. El SoC puede incluir, asimismo, componentes de conectividad tales como buses simples o redes en chip siguiendo la especificación Advanced Microcontroller Bus Architecture (AMBA) de ARM que conectan estos bloques entre sí tal como se conoce en la técnica. Algunos bloques pueden estar empaquetados por separado y estar apilados en la parte superior del SoC, un diseño conocido en la técnica como paquete sobre paquete (PoP - Package-on-Package, en inglés). Alternativamente, algunos bloques pueden estar comprendidos en distintos circuitos integrados (o sustratos) pero empaquetados juntos, un diseño conocido en la técnica como sistema en paquete (SiP – System in Packet, en inglés).

Área segura aislada del procesador: una entidad de procesamiento caracterizada por componentes específicos de hardware y/o software sujetos a una certificación que garantiza un nivel específico de seguridad, de acuerdo con estándares de seguridad específicos. El área segura aislada garantiza que los datos confidenciales sean almacenados, procesados y protegidos en un entorno seguro y fiable del procesador, a la vez que mantiene altas velocidades de procesamiento y grandes cantidades de memoria accesible. El área segura aislada puede ofrecer ejecución aislada, almacenamiento seguro, certificación remota, aprovisionamiento seguro, arranque fiable y ruta fiable. El área segura aislada permite al procesador funcionar en dos modos lógicos: mundo normal o mundo seguro. El mundo normal es ejecutado por el área no segura del procesador y puede comprender el sistema operativo enriquecido no seguro (Rich Operating System (OS), en inglés) y los componentes de software y las aplicaciones que se ejecutan sobre el OS enriquecido. El mundo normal está excluido del acceso a recursos que son aprovisionados para uso exclusivo en el mundo seguro. El mundo seguro es ejecutado por el área segura aislada, que es la única entidad que tiene acceso a los recursos aprovisionados para su uso exclusivo en el área segura, tales como ciertos rangos delineados de memoria ROM o RAM, registros de configuración de procesador o coprocesador, y ciertos periféricos, tales como controladores de pantalla o controladores de pantalla táctil, y sus registros de configuración asociados. Algunos de los recursos previstos para el uso exclusivo del área segura aislada pueden estar en el mismo sustrato o paquete que el SoC, mientras que otros pueden estar contenidos en un sustrato o paquete diferente. Algunos de los recursos pueden ser aprovisionados de manera dinámica para el uso exclusivo del área segura aislada en ciertos momentos, mientras que en otros momentos pueden estar disponibles para su uso en el mundo normal. El área segura aislada solo ejecuta aplicaciones autorizadas y fiables, y proporciona seguridad contra ataques lógicos generados en el entorno del OS enriquecido, ataques que tienen como objetivo poner en peligro el firmware de arranque, ataques que aprovechan las interfaces de depuración y prueba y otros ataques no invasivos. Ejemplos no limitativos de un área segura aislada del procesador incluyen entorno de ejecución fiable (TEE - Trusted Execution Environment, en inglés), tecnología de ejecución fiable (TXT - Trusted Execution Technology, en inglés) comercializada por la firma Intel, módulo de plataforma fiable (TPM - Trusted Platform Module, en inglés), el chip Hengzhi y el chip de subsistema de seguridad incorporado (ESS - Embedded Security Subsystem), comercializado por la firma IBM. En algunas realizaciones, el área segura aislada del procesador está diseñada para que no sea accesible, incluso por un administrador humano. En algunas realizaciones, el área segura aislada puede estar implementada parcial o completamente por medio de un elemento de hardware exclusivo tal como, pero sin estar limitado al mismo, un elemento seguro, tal como está definido en el párrafo que sigue. El experto en la materia de la presente tecnología puede idear, asimismo, otras variaciones del área segura aislada, sin apartarse del alcance de la presente tecnología.

Elemento seguro: una entidad de procesamiento caracterizada por componentes específicos de hardware y/o software sujetos a una certificación que garantiza un nivel específico de seguridad de acuerdo con estándares de seguridad específicos. Desde una perspectiva de hardware, un elemento seguro incluye los componentes habituales que se encuentran en una entidad informática: al menos un microprocesador (por ejemplo, CPU), una memoria (por ejemplo, una memoria ROM, RAM o FLASH), interfaces de comunicación, etc. Asimismo, pueden estar incluidos componentes de hardware específicos para implementar funcionalidades específicas particulares de un elemento seguro. Por ejemplo, puede estar incluido un acelerador criptográfico. Además, pueden estar incluidas diversas características de resistencia a la manipulación, detección de manipulación y/o respuesta de manipulación para impedir que una persona malintencionada extraiga información confidencial del elemento seguro. Medidas anti-sabotaje pueden incluir aspectos de hardware, aspectos de software o una combinación de hardware y software. Además, pueden estar incluidas en el

elemento seguro ciertas contramedidas para prevenir ataques de canal lateral con el objetivo de recuperar claves criptográficas u otra información confidencial. Las contramedidas contra ataques de canal lateral pueden incluir aspectos de hardware, aspectos de software o ambos. Además, pueden estar incluidas medidas para reducir las emisiones EM, tales como el apantallamiento, para proteger el elemento seguro de escuchas clandestinas. En el contexto de las transacciones financieras, la certificación del elemento seguro garantiza que varias entidades financieras estén dispuestas a utilizar el elemento seguro para almacenar y procesar datos financieros críticos, y para realizar transacciones financieras seguras utilizando los datos financieros críticos. En algunas realizaciones, el elemento seguro puede estar caracterizado únicamente por componentes de software. El elemento seguro puede estar implementado, en algunas realizaciones, parcial o completamente, como un área segura aislada del procesador, tal como el aislado seguro tal como se ha descrito en el párrafo anterior, en cuyo caso, el elemento seguro puede estar implementado, por ejemplo, pero sin ser limitativos, como un TEE, un TPM y/o un ESS. El experto en la técnica de la presente tecnología también puede idear otras variaciones del elemento seguro sin apartarse del alcance de la presente tecnología.

Pantalla táctil: un dispositivo sensor sensible al tacto con una interfaz de entrada y/o salida superpuesta, en general, en la parte superior de una pantalla visual electrónica de un sistema de procesamiento de información. Las pantallas táctiles funcionan, en general, detectando el contacto táctil y/o háptico con la pantalla táctil. Las tecnologías de pantalla táctil pueden incluir, entre otras, resistiva, onda acústica superficial, capacitiva, capacitiva proyectiva, rejilla infrarroja, proyección acrílica infrarroja, imagen óptica, tecnología de señal dispersiva y pantallas táctiles de reconocimiento de pulso acústico. Las pantallas táctiles pueden incluir componentes sensibles a la fuerza para detectar la presión aplicada a la pantalla. Las pantallas táctiles también pueden incluir componentes de retroalimentación háptica. La persona experta en la técnica de la presente tecnología también puede idear otras variaciones de la pantalla táctil sin apartarse del alcance de la presente tecnología.

Controlador de pantalla táctil: un controlador que detecta las señales táctiles analógicas emitidas por la pantalla táctil, puede realizar la conversión de analógico a digital de la salida analógica, puede realizar las etapas de procesamiento de señal para condicionar la señal y deducir las coordenadas de la pantalla asociadas con uno o más eventos de contacto táctil. Típicamente, pero no de manera limitativa, las coordenadas de los eventos táctiles serán enviadas a un procesador utilizando interfaces de serie de bajo ancho de banda, incluidas la interfaz periférica de serie (SPI – Serial Peripheral Interface, en inglés) y las interfaces de circuito inter-integrado (I^2C), tal como es conocido en la técnica. El controlador de la pantalla táctil puede estar integrado con el controlador de la pantalla o con cualquier otro bloque. La persona experta en la técnica de la presente tecnología puede imaginar, asimismo, otras variaciones del controlador de la pantalla táctil, sin apartarse del alcance de la presente tecnología.

Pantalla de visualización: un dispositivo de visualización visual electrónico con una interfaz de entrada y/o salida, utilizado para transmitir información visual al usuario. Las tecnologías de la pantalla pueden incluir, entre otras, pantallas de cristal líquido (LCD – Liquid Crystal Displays, en inglés), pantallas basadas en tecnología de diodo emisor de luz orgánico (OLED – Organic Light-Emitting Diode, en inglés), pantallas basadas en tecnología de diodo emisor de luz orgánico de matriz activa (AMOLED – Active Matrix Organic Light-Emitting Diode, en inglés).

Controlador de pantalla de visualización: un dispositivo capaz de introducir en la memoria datos de imágenes digitales, ya sea desde una memoria intermedia de fotogramas o desde una interfaz digital estándar, tal como MIPI o eDP, y emitir señales de video analógicas o digitales adecuadas para interactuar con la tecnología de pantalla específica y una velocidad de fotogramas adecuada (por ejemplo, utilizando LVDS). El controlador de la pantalla puede estar incluido en el mismo sustrato o paquete que el procesador SoC, o ser un componente discreto, o estar integrado con la pantalla de visualización, o una combinación. El controlador de la pantalla puede incluir funciones para aumentar la escala, reducir la escala, rotación y combinación de la imagen.

Interfaz de usuario de confianza (TUI – Trusted User Interface, en inglés): una combinación de software, hardware y recursos periféricos que pueden estar reservados para el uso exclusivo del área segura aislada, y pueden estar configurados de tal manera que proporcionen un control exclusivo e ininterrumpido de la pantalla de visualización (o de una parte de la misma) y del sensor táctil al área segura aislada y mantengan la integridad y confidencialidad de las imágenes mostradas y de los eventos táctiles generados por el sensor táctil y el controlador. La TUI en un dispositivo puede estar sujeta a una certificación que garantice un nivel específico de seguridad de acuerdo con estándares de seguridad específicos. Una TUI detecta automáticamente y solo permite que aplicaciones autorizadas o de confianza accedan al contenido de una memoria de pantalla segura. En una realización, la TUI es un modo específico en el que el dispositivo está controlado por el área segura aislada del procesador para garantizar que la información que se muestra en la pantalla táctil proviene de una fuente fiable y aislada del sistema operativo. La persona experta en la técnica de la presente tecnología puede idear, asimismo, otras variaciones de la TUI sin apartarse del alcance de la presente tecnología.

Información / datos: los términos “información” y “datos” se utilizan indistintamente y tienen un significado similar para el propósito de la presente invención.

Los estándares de seguridad pueden comprender múltiples niveles de seguridad, tales como, sin ser limitativos, Nivel 1, Nivel 2 o Nivel 3. Como ejemplo, pero sin ser limitativos, el Nivel 1 puede corresponder a un nivel de seguridad más alto que el Nivel 2, que, a su vez, puede corresponder a un nivel de seguridad superior al Nivel 3. Por ejemplo, pero

sin ser limitativo, el estándar EMCo puede proporcionar ejemplos de niveles de seguridad y estándares de aprobación y certificación, tales como el proceso de aprobación del tipo de terminal, el proceso de evaluación de la seguridad, el proceso de aprobación del tipo de tarjeta o el proceso de aprobación del tipo de móvil.

Por ejemplo, el proceso de aprobación del tipo de terminal puede ser un mecanismo para prueba de cumplimiento con las especificaciones Europay, MasterCard y Visa (EMV). La aprobación del tipo de terminal puede proporcionar un nivel de confianza de que se puede conseguir la interoperabilidad y el comportamiento coherente entre aplicaciones conformes. En un ejemplo, la prueba de aprobación del tipo terminal puede estar dividida en dos niveles, Nivel 1 y Nivel 2. El proceso de aprobación del tipo de Nivel 1 puede probar el cumplimiento de las características electromecánicas, la interfaz lógica y los requisitos del protocolo de transmisión definidos en las especificaciones de EMV. La aprobación de tipo de Nivel 2 puede probar el cumplimiento de los requisitos de la aplicación de débito / crédito tal como se define en las especificaciones EMV. Además, la prueba de aprobación del tipo de terminal puede incluir una aprobación de Nivel 3, que garantiza comunicaciones seguras entre una aplicación ejecutada en el terminal y una institución financiera.

Aunque los diversos componentes definidos anteriormente están asociados con una definición, se debe entender que cada uno de los diversos componentes no debe ser interpretado como limitado únicamente a las funciones y/o detalles específicos proporcionados en la definición asociada. Por el contrario, se pueden agregar, eliminar o combinar otras funciones y/o detalles específicos sin apartarse del alcance de la presente tecnología. Además, las funciones y/o los detalles pueden ser cambiados de un componente a otro componente sin apartarse del alcance de la presente tecnología (por ejemplo, una función asociada con la pantalla táctil puede ser cambiada al controlador de pantalla táctil). Algunos de los diversos componentes también pueden estar fusionados parcial o completamente sin apartarse del alcance de la presente tecnología (por ejemplo, la pantalla táctil y el controlador de la pantalla táctil pueden estar fusionados para definir un solo componente, o el controlador de la pantalla y el procesador pueden estar fusionados para definir un solo componente).

La figura 1 es un diagrama de bloques que ilustra diversos componentes y características a modo de ejemplo de un dispositivo ilustrativo 100, de acuerdo con una realización de la presente tecnología.

De acuerdo con, al menos, una realización descrita en el presente documento, se proporcionan un método y un sistema para realizar una transacción financiera segura en un dispositivo. El dispositivo comprende un procesador, el procesador comprende un área segura aislada, una pantalla de visualización conectada operativamente a un controlador de pantalla de visualización, estando conectado el controlador de la pantalla de visualización operativamente al procesador, una pantalla táctil conectada operativamente a un controlador de pantalla táctil, estando conectado el controlador de la pantalla táctil operativamente al procesador y a un elemento seguro asociado con el procesador.

En algunas realizaciones, el dispositivo puede estar implementado como cualquier dispositivo que comprenda los componentes necesarios para contener un método y un sistema que se detallan a continuación en el presente documento. En algunas realizaciones, el dispositivo puede incluir un teléfono inteligente, un phablet, un reloj inteligente y/o un ordenador portátil, un PDA, una tableta y un ordenador. En algunas realizaciones alternativas, el dispositivo también puede estar incrustado en o sobre objetos no exclusivamente dedicados al cálculo y/o a funciones de procesamiento de información, tales como, entre otros, un vehículo, un mueble, un electrodoméstico, etc.

En la realización ilustrada, el dispositivo 100 comprende un paquete móvil 110 de chipset de paquete (PoP), un panel táctil capacitivo proyectivo superpuesto en una pantalla LCD 130, un controlador de pantalla y un controlador de pantalla táctil 140, un elemento seguro y un extremo frontal sin contacto 150 y una memoria flash 120.

En una realización no limitativa, el chipset móvil de PoP 110 comprende una memoria 112 de doble velocidad de datos baja potencia (LP DDR – Low Power Double Data Rate, en inglés) apilada con un procesador de aplicación de SoC 114. El procesador de aplicación de SoC 114 comprende un área segura aislada (ISA – Isolated Secured Area, en inglés) 115, una unidad central de procesamiento (CPU) 116, una interfaz de usuario fiable (TUI) 117, una memoria de solo lectura (ROM – Read Only Memory, en inglés) 118 segura y una memoria de acceso aleatorio (RAM – Random Access Memory, en inglés) 119 segura. La LP DDR 112 comprende una memoria RAM 113 segura. El chipset móvil de PoP 110 está conectado a una memoria flash 120 que comprende objetos seguros 122.

En algunas realizaciones de la presente tecnología, el dispositivo puede ejecutar un sistema operativo (OS) no seguro. Ejemplos de un sistema operativo que es ejecutado en el procesador de aplicaciones SoC 114 incluyen, entre otros, una versión de iOS® o un derivado de la misma, comercializada por la firma Apple Inc.; una versión del OS® de Android, o un derivado del mismo, comercializada por la firma Google Inc.; una versión del OS® de PlayBoo, o un derivado de la misma, comercializada por la firma RIM Inc. Se comprende que otros sistemas operativos propietarios o sistemas operativos personalizados pueden ser utilizados por igual sin apartarse del alcance de la presente tecnología.

En algunas realizaciones de la presente tecnología, el área segura aislada puede ejecutar un sistema operativo seguro, que es independiente, distinto y está aislado del sistema operativo que ejecuta el área no segura del procesador. El OS seguro típicamente tiene niveles de privilegios más altos que el OS no seguro, lo que le permite, por ejemplo,

excluir al OS no seguro del acceso a recursos confidenciales. El OS seguro puede ser completamente diferente del OS no seguro (por ejemplo, un microkernel seguro), o puede ser sustancialmente el mismo que el OS no seguro (por ejemplo, una versión modificada del OS Android C).

El controlador de la pantalla táctil 144 está conectado a la interfaz de usuario 116 fiable por medio de una interfaz periférica en serie (SPI) o interfaz de circuito inter-integrado (i^2C), interfaces de serie conocidas en la técnica para conectar circuitos integrados (IC – Integrated Circuits, en inglés) a procesadores y microcontroladores. El controlador de la pantalla táctil 144 está conectado a la interfaz de usuario 116 fiable y al controlador de pantalla 142 con una interfaz de serie de la pantalla MIPI (MIPI-DSI – MIPI Display Serial Interface, en inglés) o una conexión de puerto de pantalla integrado (eDP – Embedded Display Port, en inglés), protocolos de comunicación y buses de serie entre el anfitrión y el dispositivo, tal como sería reconocido por alguien experto en la materia. El panel táctil capacitivo proyectivo 134 está superpuesto en la pantalla LCD 132. El elemento seguro 152 está conectado al procesador de aplicación de SoC 114 por medio de una interfaz de bus SPI. El extremo frontal sin contacto 140 está conectado al procesador de aplicación de SoC 114 con una interfaz i^2C. En algunas realizaciones, el controlador de la pantalla táctil 144 puede estar conectado de manera segura a la TUI 117, de modo que cada transmisión de datos entre el controlador de la pantalla táctil 144 y la TUI 117 está encriptada. En algunas realizaciones, el elemento seguro 152 está conectado de manera segura al extremo frontal sin contacto 154 y al procesador de aplicación de SoC 114, de modo que cada transmisión de datos entre el elemento seguro 152, el extremo frontal sin contacto 152 y el procesador de aplicación de SoC está encriptada. Dichos ejemplos de dispositivos y conexiones solo se presentan con fines ilustrativos, y pueden ser posibles otras variaciones, como reconocería un experto en la materia de la presente tecnología.

Volviendo a continuación a la figura 2a, se ilustra un ejemplo no limitativo de una tabla de correspondencia 200. En algunas realizaciones, la tabla de correspondencia 200 puede ser una matriz. Cada columna de la tabla de correspondencia 200 puede representar una posición 202 en un teclado. Asociado con cada posición 202 está dispuesto un valor 204. En algunas realizaciones, un generador de número pseudoaleatorio (PRNG – PseudoRandom Number Generator, en inglés) puede generar cada valor 204, de modo que cada valor tiene solo una aparición en la tabla de correspondencia 200, y cada valor tiene la misma probabilidad de aparecer en una posición dada. La tabla de correspondencia 200 puede ser utilizada, por lo tanto, para generar un teclado aleatorizado, tal como el teclado aleatorizado de la figura 2c. Pueden ser posibles otras realizaciones de la tabla de correspondencia, donde los valores son reemplazados por letras o símbolos, como reconocería alguien experto en la materia. En algunas realizaciones, la tabla de correspondencia, una vez generada, puede ser enviada al elemento seguro para la reconstitución posterior de un PIC.

Volviendo a continuación a la figura 2b, se ilustra un ejemplo no limitativo de una representación gráfica de una distribución de los puntos de conexión 240. La distribución de los puntos de conexión 240 corresponde a la geometría y la posición de cada tecla que puede ser pulsada por un usuario en una pantalla táctil. Como ejemplo no limitativo, la distribución de los puntos de conexión puede definir que la tecla 245, que representa la posición 1 en el teclado, corresponde a cada evento táctil cuya coordenada se encuentra dentro del rectángulo definido por las coordenadas 242 y 244. La distribución de los puntos de conexión 240 puede ser enviada a un controlador de pantalla táctil, y el controlador de la pantalla táctil puede procesar un evento táctil incluso de acuerdo con la distribución de los puntos de conexión, para generar un evento de codificación.

Volviendo a continuación a la figura 2c, se ilustra un ejemplo no limitativo de una representación visual de un teclado aleatorizado 280 codificado. La representación visual de un teclado aleatorizado 280 con valores 285 puede ser generada combinando la información en una tabla de correspondencia 220 y una distribución de los puntos de conexión 240. En otras realizaciones, el teclado aleatorizado 280 puede ser generado mediante otros tipos de tablas de correspondencia y distribuciones de los puntos de conexión. Se comprende que el teclado aleatorizado 280 solo se presenta como un propósito ilustrativo, y otras formas y disposiciones de un teclado aleatorizado pueden ser posibles, como sería reconocido por alguien experto en la materia. En algunas realizaciones, el teclado aleatorizado 280 puede formar parte de una pantalla de introducción del PIC tal como la pantalla de introducción del PIC de la figura 3, y ser transmitido para ser mostrado en una pantalla mediante un controlador de pantalla.

Un teclado aleatorizado proporciona un cierto nivel de seguridad para la introducción del PIC, puesto que hace que el proceso de observación directa del PIC por parte de una persona o software malicioso sea más molesto. Incluso si una persona o software malicioso tiene acceso a la salida del evento táctil o a los eventos de codificación, es imposible reconstituir el PIC sin conocer la tabla de correspondencia del teclado aleatorizado. Una nueva aleatorización del teclado después de cada evento táctil puede añadir un nivel adicional de seguridad.

Volviendo a continuación a la figura 3, se ilustra una realización no limitativa de una pantalla de introducción del código de identificación personal (PIC) para realizar una transacción segura. En una realización de la presente tecnología, el PIC es un número de identificación personal (PIN). La pantalla de introducción del PIN puede formar parte de una aplicación o software ejecutado por la CPU y/o el área segura aislada del procesador del dispositivo. En otras realizaciones, la pantalla de introducción del PIN puede formar parte de una aplicación independiente, una extensión de otra aplicación, o puede ser llamada por una llamada de procedimiento desde otra aplicación cuando se necesita una introducción segura del PIN. La pantalla de introducción del PIN 300 puede ser mostrada en una parte de la pantalla o en toda la pantalla, y puede ser ejecutada paralelamente a otra aplicación que aparece en una parte diferente

de la pantalla. En esta realización, se muestra un logotipo 310 en la parte superior de la pantalla de introducción del PIN 300. Se muestra un texto que solicita al usuario que introduzca su PIN 320 debajo del logotipo 310. El campo de introducción de datos 330, con asteriscos correspondientes a las teclas pulsadas por el usuario en la pantalla táctil se muestra debajo del texto de solicitud 320. Un teclado aleatorizado 340 se muestra debajo del campo de introducción de datos 330, con los botones de confirmación y validación 350 correctos. Un indicador de seguridad 360 asociado con el usuario se muestra en la parte inferior de la pantalla. El indicador de seguridad 360 comprende un secreto compartido entre el usuario y una entidad fiable, tal como, entre otros, una institución financiera que posee su cuenta. El secreto compartido puede ser una imagen, un eslogan o cualquier otra información secreta reconocida por el usuario, y se muestra para que el usuario pueda estar seguro de que está introduciendo su PIC en una aplicación fiable conectada de manera segura a un servidor fiable de su institución financiera. El indicador de seguridad 360 puede ser una transmisión de video en la que cada fotograma contiene una parte del indicador de seguridad, de tal modo que una persona o un software malicioso no puede reproducir el indicador de seguridad de una sola fotografía o captura de pantalla. En algunas realizaciones, el teclado aleatorizado puede estar compuesto de diferentes símbolos y/o números y/o letras. En realizaciones alternativas, el indicador de seguridad puede ser visual y/o auditivo y/u olfativo y/o táctil, siempre que el dispositivo tenga la tecnología requerida para soportar dichas realizaciones. Este ejemplo es solo para fines ilustrativos, y se pueden definir muchas versiones de una pantalla de introducción del PIC, como apreciaría una persona experta en la técnica de la presente tecnología.

La figura 4 es una representación de diagrama de flujo de un flujo de comunicación entre un área aislada segura del procesador de aplicación de SoC 404, un controlador de pantalla 406, un controlador de pantalla táctil 408 y un elemento seguro 402, de acuerdo con una realización del método y sistemas de la presente tecnología. En otras realizaciones de la presente tecnología, el controlador de la pantalla 406 y el controlador de la pantalla táctil 408 pueden estar fusionados en un único componente. En otras realizaciones, la función del elemento seguro puede ser desempeñada por un servidor seguro en la nube. En esta realización, el área segura aislada del procesador 404 de aplicación de SoC genera una tabla de correspondencia, una imagen de un teclado aleatorizado y coordenadas para delimitar cada tecla en el teclado aleatorizado, también conocido como distribución de los puntos de conexión en la técnica. El procesador de aplicación de SoC 404 transmite la imagen del teclado aleatorizado al controlador de pantalla 406. El procesador de aplicación de SoC 404 transmite la distribución de los puntos de conexión al controlador de pantalla táctil 408. El procesador de aplicación de SoC 404 encripta y transmite la tabla de correspondencia al elemento seguro 402.

En otras realizaciones, una TUI controlada por el área segura aislada del procesador de aplicación de SoC 404 puede generar una tabla de correspondencia, una distribución de los puntos de conexión, una imagen del teclado aleatorizado, y transmitir la imagen del teclado aleatorizado al controlador de pantalla 406, la distribución de los puntos de conexión al controlador de pantalla táctil 408 y la tabla de correspondencia al elemento seguro 402. En realizaciones alternativas, el elemento seguro 402 puede generar una tabla de correspondencia, una distribución de los puntos de conexión, una imagen del teclado aleatorizado y transmitir la imagen del teclado aleatorizado al controlador de pantalla 406 y la distribución de los puntos de acceso al controlador de pantalla táctil 408. El controlador de la pantalla táctil 408, después de haber recibido la distribución de los puntos de conexión y, por lo tanto, tener conocimiento de la ubicación y dimensiones de las teclas definidas por el área segura aislada del procesador 404, pero no de su valor, puede procesar las entradas de eventos táctiles por un usuario con la distribución de los puntos de conexión para crear uno o más eventos de codificación y encriptar los eventos de codificación resultantes. El controlador de la pantalla táctil 408 puede enviar los eventos de codificación encriptados al elemento seguro 402. En algunas realizaciones, el controlador de la pantalla táctil 408 está conectado directamente al elemento seguro 402. En otras realizaciones, el controlador de la pantalla táctil 408 puede enviar eventos de codificación encriptados al área segura aislada del procesador de aplicación de SoC 404, y el área segura aislada 404 puede enviar los eventos de codificación encriptados al elemento seguro 408. Finalmente, el elemento seguro 402 puede desencriptar los eventos de codificación encriptados y la tabla de correspondencia encriptada para reconstituir un PIC. En algunas realizaciones, el elemento seguro 402 es el único componente capaz de desencriptar la tabla de correspondencia encriptada y los eventos de codificación encriptados. En otras realizaciones, el elemento seguro 402 es el único componente que puede reconstituir un PIC a partir de versiones sin encriptar de la tabla de correspondencia y de los eventos de codificación. En realizaciones alternativas, el elemento seguro 402 es el único componente que tiene acceso a una versión sin encriptar del PIC. Después de reconstituir el PIC, el elemento seguro 402 puede encriptar el PIC reconstituido, y transmitir el PIC encriptado al área segura aislada 404. En algunas realizaciones, después de reconstituir el PIC, el PIC puede ser combinado con otra información, antes de encriptar el PIC junto con la otra información. Por ejemplo, en el contexto de las transacciones financieras, el PIN puede ser combinado con un número de cuenta personal (PAN – Personal Account Number, en inglés) para formar un bloque de PIN, según lo especificado por la norma ISO 9564. Después de que el PIC encriptado es transmitido al área segura aislada, el área segura aislada puede transmitir el PIC encriptado, a través de Internet o de otras redes, a la institución financiera que posee la cuenta del usuario, posiblemente a través de las interfaces de comunicaciones del área no segura del procesador, para que la transacción pueda ser autorizada.

Habiendo descrito, con referencia a la figura 1 a la figura 4, algunos ejemplos no limitativos de sistemas y métodos implementados por ordenador utilizados en relación con el problema de realizar una transacción utilizando un PIC, a continuación, se describirán soluciones generales al problema con referencia a la figura 5.

De manera más específica, la figura 5 muestra un diagrama de flujo que ilustra un primer método 500 implementado por ordenador para realizar una introducción segura del PIC en un dispositivo. En algunas realizaciones, la introducción segura del PIC se refiere a una transacción financiera segura utilizando un dispositivo móvil. En algunas realizaciones, el primer método implementado por ordenador 500 puede ser implementado (total o parcialmente) en el dispositivo móvil 100.

El método 500 se inicia con una etapa 502 con la generación de una tabla de correspondencia, una distribución de los puntos de conexión y una imagen del teclado aleatorizado, tal como, pero sin estar limitada a, la tabla de correspondencia de la figura 2a, la distribución de los puntos de conexión de la figura 2b y la imagen del teclado aleatorizado de la figura 2c. En algunas realizaciones, la tabla de correspondencia, la distribución de los puntos de conexión y la imagen del teclado aleatorizado pueden ser generados en el área segura aislada del procesador 115. En realizaciones alternativas, la tabla de correspondencia, el diseño de los puntos de conexión y la imagen del teclado aleatorizado pueden ser generados en un elemento seguro 152. En otras realizaciones, la tabla de correspondencia, la distribución de los puntos de conexión y la imagen del teclado aleatorizado pueden ser generados mediante un módulo externo seguro y transmitidos de manera segura a un área segura aislada del procesador 115. En algunas realizaciones, la tabla de correspondencia, la distribución de los puntos de conexión y la imagen del teclado aleatorizado pueden ser generados por un dispositivo o servidor externo, encriptados y enviados por una red de comunicación al dispositivo. De acuerdo con realizaciones alternativas de la presente tecnología, se pueden generar una o más tablas de correspondencia, la distribución de los puntos de conexión e imágenes del teclado aleatorizado al mismo tiempo. Según otras realizaciones, se pueden generar una o más tablas de correspondencia, las distribuciones de los puntos de conexión e imágenes del teclado aleatorizado en diferentes momentos.

En general, pero no de manera limitativa, para generar un teclado aleatorizado, primero se crea una tabla o matriz de correspondencia, donde el tamaño de la matriz corresponde al número de teclas en el teclado. Cada posición en la matriz, de 0 a 9, tiene como valor un número aleatorio, de modo que cada número de 0 a 9 aparece solo una vez como un valor en la matriz. Por lo tanto, se puede generar una imagen del teclado aleatorizado a partir de la matriz de correspondencia, donde cada posición de tecla tiene el valor correspondiente. Asimismo, se puede generar una distribución de los puntos de conexión, donde están definidas la ubicación y la geometría de las teclas accionables. En algunas realizaciones, la geometría y la posición de la distribución de los puntos de conexión pueden ser aleatorizados y/o codificados, asimismo, y pueden ser encriptados adicionalmente. Pueden ser posibles diferentes métodos para generar la tabla de correspondencia, la distribución de los puntos de conexión y la imagen del teclado aleatorizado, como reconocería alguien experto en la técnica de la presente tecnología.

La imagen del teclado aleatorizado puede estar integrada en una pantalla de introducción del PIC, tal como la pantalla de introducción del PIC de la figura 3. Se puede generar una representación visual de un teclado aleatorizado en forma de una imagen. En otra realización de la presente tecnología, el teclado aleatorizado puede ser generado en forma de secuencia de video, donde cada fotograma individual del video contiene una parte del teclado, y la rápida sucesión de fotogramas hace que el video aparezca como una imagen estática para el ojo humano. Esto puede agregar una capa de seguridad, al hacer que el proceso de capturar el teclado aleatorizado mediante la fotografía del dispositivo o la captura de pantalla sea más molesto, ya que ningún fotograma contiene suficiente información para reconstruir el teclado aleatorizado y, de este modo, obtener un conocimiento de la tabla de correspondencia.

A continuación, en la etapa 504, la tabla de correspondencia del teclado aleatorizado es transmitida al elemento seguro 152. En algunas realizaciones, la correspondencia puede ser encriptada antes de ser transmitida al elemento seguro 152

A continuación, en la etapa 506, la imagen del teclado aleatorizado es transmitida a un controlador de pantalla 142. En algunas realizaciones, se pueden transmitir una pluralidad de pantallas de introducción del PIC diferentes que comprenden diferentes teclados aleatorizados al controlador de pantalla 142. En otras realizaciones, una TUI 117 puede generar la tabla de correspondencia, la distribución de los puntos de conexión, la imagen del teclado aleatorizado y transmitir la imagen del teclado aleatorizado al controlador de pantalla 142. En algunas realizaciones, la pantalla de introducción del PIC puede comprender un indicador de seguridad. En otras realizaciones, la imagen del teclado aleatorizado es transmitida desde el elemento seguro al área segura aislada antes de ser transmitida al controlador de pantalla 142. En realizaciones alternativas, la tabla de correspondencia, la distribución de los puntos de conexión y la imagen del teclado aleatorizado pueden ser generados en el elemento seguro 115, estando conectado el elemento seguro 115 directamente al controlador de pantalla 142, y, a continuación, transmitidos al controlador de pantalla.

En una etapa 508, la distribución de los puntos de conexión es transmitida al controlador de pantalla táctil. En algunas realizaciones, la distribución de los puntos de conexión es generada en el área segura aislada del procesador y transmitida al controlador de pantalla táctil. En otras realizaciones, la distribución de los puntos de conexión es generada en el elemento seguro, encriptada y transmitida al controlador de pantalla táctil.

En una etapa 510, el controlador de la pantalla 142 hace que se muestre la imagen del teclado aleatorizado en la pantalla de visualización 132. La imagen del teclado aleatorizado puede ser mostrada en cualquier parte de la pantalla de visualización 132. En algunas realizaciones, cada tecla de la imagen del teclado aleatorizado puede ser mostrada

en las teclas físicas correspondientes que comprenden pantallas incrustadas. En otras realizaciones, se puede mostrar un indicador de seguridad al mismo tiempo que el teclado aleatorizado.

En una etapa 512, el controlador de la pantalla táctil 144 detecta una o más entradas de eventos táctiles en la pantalla táctil 134 de un usuario. Las entradas de eventos táctiles pueden ser introducidas por un usuario con los dedos, con un puntero / lápiz, o con cualquier cosa que pueda ser detectada por la pantalla táctil 134. Como ejemplo no limitativo, la pantalla táctil 134 puede utilizar tecnología capacitiva proyectada (p-cap) para detectar una entrada, en donde los sensores capacitivos detectan cualquier cosa que sea conductiva o que tenga una constante dieléctrica diferente del aire. Los sensores capacitivos comprenden electrodos individuales o intersecciones de electrodos que son escaneados de manera repetida e iterativa por un controlador de pantalla táctil para detectar cambios en la capacitancia. Se puede determinar una coordenada táctil x-y precisa con un estado correspondiente (por ejemplo, tocar o soltar) interpolando valores de capacitancia de múltiples electrodos o intersecciones adyacentes. En algunas realizaciones, la pantalla táctil 134 también puede comprender sensores de presión para detectar diferentes niveles de presión. En realizaciones alternativas, el teclado que se muestra en la pantalla puede volver a ser aleatorizado o cambiado a un diseño diferente por el área segura aislada del procesador 115 después de cada entrada de evento táctil, de modo que aparece un teclado aleatorizado diferente después de cada entrada táctil por parte del usuario. En una realización alternativa, un ratón, un panel táctil o una pantalla táctil pueden ser conectados al dispositivo, y los eventos correspondientes pueden ser procesados en un controlador de pantalla táctil o en un área segura aislada del procesador.

En una etapa 514, un controlador de pantalla táctil 144 genera uno o más eventos de codificación en base a las entradas de eventos táctiles por parte del usuario en la etapa 512. El controlador de la pantalla táctil, en primer lugar, procesa las entradas de eventos táctiles analógicas por parte del usuario en salidas de eventos táctiles digitales. La generación de salidas de eventos táctiles basadas en entradas de eventos táctiles por parte de un usuario en una pantalla táctil es bien conocida en la técnica de la presente tecnología. En algunas realizaciones, también se puede generar una coordenada táctil z si la pantalla táctil 134 comprende un sensor de presión. En realizaciones alternativas, el controlador de la pantalla táctil 144 puede descartar cada gesto que no sea una sola entrada táctil, tal como, entre otros, gestos de deslizamiento o gestos multitáctiles. En algunas realizaciones, múltiples salidas de eventos táctiles pueden corresponder a un solo evento de codificación. Las coordenadas de salida del evento táctil pueden ser convertidas en eventos de codificación comparándolas con la distribución de los puntos de conexión, en donde un evento táctil puede corresponder a la posición “2” en el teclado aleatorizado, porque la coordenada de salida del evento táctil cae dentro de los límites del punto de conexión en la posición “2”.

En una etapa 516, el controlador de la pantalla táctil 144 encripta los uno o más eventos de codificación generados en la etapa 514. En algunas realizaciones, los uno o más eventos de codificación pueden ser encriptados utilizando criptografía asimétrica, mientras que en otras realizaciones se puede utilizar criptografía simétrica. En algunas realizaciones, se pueden utilizar encriptadores de bloque, mientras que en otras realizaciones se pueden utilizar encriptadores de flujo. En otras realizaciones adicionales, se puede utilizar criptografía de caja blanca. Si se utiliza criptografía asimétrica, los eventos de codificación pueden ser encriptados mediante una clave criptográfica pública o privada. Algunas realizaciones pueden emplear el algoritmo RSA, mientras que otras realizaciones pueden emplear algoritmos basados en curvas elípticas, el problema del logaritmo discreto u otros principios matemáticos. Si se utiliza criptografía simétrica, la clave es secreta y el algoritmo de encriptado puede ser DES, TDES o AES u otros métodos de encriptado conocidos en la técnica. En algunas realizaciones, el controlador de la pantalla táctil puede encriptar los eventos táctiles de acuerdo con los estándares de seguridad de encriptado de la industria financiera. En algunas realizaciones, la clave utilizada puede ser cambiada para cada transacción y ser única para cada dispositivo. De manera más específica, la clave puede ser cambiada de acuerdo con las especificaciones ANSI X9.24 y el método de Clave Única Dinámica por Transacción (DUKPT – Dynamic Unique Key Per Transaction, en inglés).

En la etapa 518, el controlador de la pantalla táctil 144 transmite los eventos de codificación encriptados de la etapa 516. En algunas realizaciones, el controlador de la pantalla táctil 144 transmite los eventos de codificación encriptados al elemento seguro 152. En otras realizaciones, el controlador de la pantalla táctil 144 puede ser conectado directamente al elemento seguro 152. En realizaciones alternativas, el controlador de la pantalla táctil puede transmitir los eventos de codificación encriptados al área segura aislada del procesador 115, y los eventos de codificación encriptados pueden ser transmitidos, a continuación, al elemento seguro 152 por el área segura aislada del procesador.

Son posibles diversos ordenamientos adicionales de algunas de las etapas de la figura 5, tal como será fácilmente evidente para alguien experto en la técnica. Por ejemplo, en algunas realizaciones, la etapa 504 puede ser ejecutada después de la etapa 506 y/o la etapa 508. En algunas realizaciones, las etapas 504 y 518 pueden ser ejecutadas al mismo tiempo. En otras realizaciones, la etapa 504 puede ser ejecutada después de la etapa 518.

En la etapa 520, el elemento seguro 152 desencripta los eventos de codificación encriptados. En algunas realizaciones, los eventos de codificación encriptados pueden ser desencriptados utilizando una clave criptográfica privada. En las realizaciones en las que la tabla de correspondencia del teclado aleatorizado ha sido encriptada previamente, es desencriptada antes, después o al mismo tiempo que los eventos táctiles encriptados.

En una etapa 522, el elemento seguro 152 reconstituye el PIC asociado con el usuario en base a uno o más eventos de codificación y a la tabla de correspondencia del teclado aleatorizado. En algunas realizaciones, el PIC es reconstituido ejecutando una función que genera el PIC encontrando los valores correspondientes a la posición de los eventos de codificación. Estudiando la tabla de correspondencia, esta función puede determinar que el evento de codificación correspondiente a “2” está asociado con un valor 5. La función puede determinar que un evento de codificación corresponde a una entrada de PIC de 5. Este ejemplo se proporciona solo como un ejemplo ilustrativo para reconstituir el PIC, y es uno de los posibles métodos para determinar los eventos de codificación correspondientes, ya que puede ser reconocido por una persona experta en la técnica de la presente tecnología.

En algunas realizaciones, el PIC reconstituido es encriptado por el elemento seguro. En algunas realizaciones, el PIC encriptado es transmitido al área segura aislada del procesador después de ser encriptado por el elemento seguro. El PIC encriptado puede ser enviado a través de una red de comunicación a un servidor remoto para finalizar la transacción. En realizaciones alternativas en las que la tabla de correspondencia ha sido encriptada previamente, la tabla de correspondencia encriptada del teclado aleatorizado y los eventos de encriptado pueden ser enviados a un servidor remoto antes de ser desencriptados y reconstituidos a un PIC por el servidor remoto. En realizaciones alternativas, se le puede solicitar al usuario que proporcione un método adicional de autenticación, que incluye, entre otros, datos biométricos, un segundo PIC o cualquier otra información legible por ordenador asociada con el usuario.

El presente método y sistemas pueden ser utilizados en diferentes contextos no limitativos. Una utilización a modo de ejemplo es durante una transacción financiera entre un cliente y un comerciante, donde un dispositivo móvil tal como un teléfono o tableta implementa el método y el sistema y el comerciante puede utilizarlo como terminal de pago. El cliente puede tocar su tarjeta en el dispositivo para realizar un pago, comprendiendo la tarjeta un chip de RFID o NFC, comprendiendo también el dispositivo una interfaz de RFID o NFC para comunicarse con la tarjeta. El dispositivo puede presentar una pantalla de introducción del PIC con un indicador de seguridad asociado con el usuario y solicitar al usuario que introduzca su PIC para confirmar la transacción. En algunas realizaciones, el cliente puede recibir una confirmación de la transacción del comerciante y/o la institución financiera que posee una cuenta relevante asociada con el cliente.

Otra utilización a modo de ejemplo es durante una transacción de igual a igual, donde una primera persona que posee una tarjeta de pago podría transferir fondos a una segunda persona que posee un dispositivo móvil. La primera persona podría tocar con su tarjeta el dispositivo móvil de la segunda persona, comprendiendo la tarjeta un chip de RFID o NFC, comprendiendo también el dispositivo una interfaz de RFID o NFC para comunicarse con la tarjeta. La segunda persona puede presentar el dispositivo con una pantalla de introducción del PIC que comprende un indicador de seguridad asociado con la primera persona, y solicitar a la primera persona que introduzca su PIC para confirmar la transacción. El pago también podría hacerse de la manera opuesta, donde los fondos son transferidos desde el dispositivo de la segunda persona a la tarjeta de la primera persona, en cuyo caso la segunda persona introduce su propio PIC en su propio dispositivo.

Otra utilización a modo de ejemplo es durante una transacción entre dos personas, teniendo las dos personas dispositivos habilitados para NFC o RFID. Las dos personas podían intercambiar fondos aproximando sus dispositivos uno a otro. Alternativamente, las dos personas podrían iniciar y realizar la transacción a distancia a través de una red de comunicaciones. En cualquier caso, para confirmar la transacción, al menos una persona puede recibir una pantalla de confirmación del PIC para completar la transacción.

Especialmente, las características y ejemplos anteriores no pretenden limitar el alcance de la invención actual a una sola realización, puesto que otras realizaciones son posibles mediante el intercambio de algunos o todos los elementos descritos o ilustrados. Además, cuando ciertos elementos de la presente invención pueden ser implementados parcial o totalmente utilizando componentes conocidos, solo se describen las partes de dichos componentes conocidos que son necesarias para comprender la presente invención, y se omiten descripciones detalladas de otras partes de dichos componentes conocidos, para no oscurecer la invención. En la presente memoria descriptiva, una realización que muestra un componente singular no debe estar limitada necesariamente a otras realizaciones que incluyen una pluralidad del mismo componente, y viceversa, a menos que se indique explícitamente lo contrario en el presente documento. Además, los solicitantes no pretenden que se atribuya a ningún término en la memoria descriptiva o afirmación un significado especial o poco común, a menos que se establezca explícitamente de este modo. Además, la presente invención abarca los equivalentes conocidos presentes y futuros de los componentes conocidos a los que se hace referencia en este documento a modo de ilustración.

La descripción anterior de las realizaciones específicas da a conocer completamente la naturaleza general de la invención que otros pueden modificar y/o adaptar fácilmente, aplicando el conocimiento dentro de la habilidad de la técnica o las técnicas relevantes (incluyendo el contenido de los documentos citados e incorporados como referencia en este documento), para diversas aplicaciones, tales formas de realización específicas, sin experimentación indebida y sin apartarse del concepto general de la presente invención. Por lo tanto, dichas adaptaciones y modificaciones están previstas para estar dentro del significado y el rango de equivalentes de las realizaciones descritas, en base a la explicación y orientación presentadas en el presente documento. Se debe entender que la fraseología o terminología en el presente documento tiene el propósito de descripción y no de limitación, de modo que la terminología o fraseología de la presente memoria descriptiva debe ser interpretada por el experto en la materia a la luz de las

explicaciones y orientación presentadas en el presente documento, en combinación con el conocimiento de un experto en la técnica o las técnicas relevantes.

Si bien las implementaciones descritas anteriormente se han descrito y mostrado con referencia a etapas particulares realizadas en un orden particular, se comprenderá que estas etapas pueden ser combinadas, subdivididas o reordenadas sin apartarse de las explicaciones de la presente tecnología. Las etapas pueden ser ejecutadas en paralelo o en serie. En consecuencia, el orden y la agrupación de las etapas no es una limitación de la presente tecnología.

Aunque se han descrito anteriormente diversas realizaciones de la presente invención, se debe entender que se han presentado a modo de ejemplo, y no de limitaciones. Sería evidente para un experto en la técnica o las técnicas relevantes que se podrían realizar diversos cambios en la forma y el detalle sin apartarse del alcance de la invención. Por lo tanto, la presente invención no debe estar limitada por ninguna de las realizaciones a modo de ejemplo descritas anteriormente, sino que debe estar definida solo de acuerdo con las siguientes reivindicaciones.

REIVINDICACIONES

1. Un método para accionar un dispositivo (100), comprendiendo el dispositivo (100) un procesador (114), comprendiendo el procesador (114) un área segura aislada (115), una pantalla de visualización (130) conectada operativamente a un controlador de pantalla (142), estando conectado el controlador de la pantalla (142) operativamente al procesador (114), una pantalla táctil (134) conectada operativamente a un controlador de pantalla táctil (144), estando conectado el controlador de la pantalla táctil (144) operativamente al procesador (114), y un elemento seguro (152) asociado con el procesador (114), comprendiendo el método:

generar una tabla de correspondencia, una distribución de los puntos de conexión y una representación visual de un teclado aleatorizado, asociando la tabla de correspondencia las posiciones de las teclas en el teclado aleatorizado y los valores, definiendo la distribución de los puntos de conexión geometrías y ubicaciones de las posiciones de las teclas en el teclado aleatorizado para ser pulsadas en la pantalla táctil (134), comprendiendo la representación visual del teclado aleatorizado los valores;

transmitir, al elemento seguro (152), la tabla de correspondencia;

transmitir, al controlador de pantalla (142), la representación visual del teclado aleatorizado;

transmitir, al controlador de la pantalla táctil (144), la distribución de los puntos de conexión;

haciendo que el controlador de la pantalla (142) muestre la representación visual del teclado aleatorizado en la pantalla (130);

detectar, mediante el controlador de la pantalla táctil (144), una entrada de evento de toque de un usuario en la pantalla táctil (134);

generar, mediante el controlador de la pantalla táctil (144), un evento de codificación en base a la entrada de evento táctil y a la distribución de los puntos de conexión, identificando el evento de codificación la tecla correspondiente en el teclado aleatorizado pulsada por el usuario en la pantalla táctil (134);

encriptar, mediante el controlador de la pantalla táctil (144), el evento de codificación;

transmitir, al elemento seguro (152), el evento de codificación encriptado;

desencriptar, mediante el elemento seguro (152), el evento de codificación encriptado; y

reconstituir, mediante el elemento seguro (152), un código de identificación personal (PIC) asociado con el usuario en base al evento de codificación y a la tabla de correspondencia, recuperando el valor de la tabla de correspondencia correspondiente al evento de codificación.

2. El método de la reivindicación 1, que comprende, además, antes de transmitir, al elemento seguro (152), la tabla de correspondencia, encriptar la tabla de correspondencia.

3. El método de la reivindicación 2, que comprende, además, después de encriptar la tabla de correspondencia, desencriptar, mediante el elemento seguro (152), la tabla de correspondencia.

4. El método de cualquiera de las reivindicaciones 1 a 3, en el que el área segura aislada (115) del procesador (114) comprende una interfaz de usuario (117) fiable.

5. El método de cualquiera de las reivindicaciones 1 a 4, en el que el método comprende, además, volver a aleatorizar, al menos, una parte de la representación visual del teclado aleatorizado, modificando la tabla de correspondencia después de que ocurra un evento de codificación.

6. El método de cualquiera de las reivindicaciones 1 a 5, en el que se generan múltiples tablas de correspondencia, distribuciones de los puntos de conexión y representaciones visuales de teclados aleatorizados antes de que ocurra un evento táctil.

7. El método de cualquiera de las reivindicaciones 1 a 6, en el que la representación visual del teclado aleatorizado es, al menos, una de una imagen y una secuencia de video.

8. El método de cualquiera de las reivindicaciones 1 a 7, en el que el método comprende, además, hacer que el controlador de la pantalla (142) muestre un indicador de seguridad previamente asociado con el usuario.

9. El método de la reivindicación 8, en el que el indicador de seguridad previamente asociado con el usuario es almacenado en el área segura aislada (115) del procesador (114).

10. El método de cualquiera de las reivindicaciones 1 a 9, que comprende, además:

encriptar el PIC reconstituido mediante el elemento seguro (152); y

transmitir el PIC reconstituido encriptado al procesador (114).

11. El método de cualquiera de las reivindicaciones 1 a 10, en el que el elemento seguro (152) es, al menos, uno de un elemento de hardware conectado operativamente al procesador (114), un componente de software ejecutado por el procesador (114), el área segura aislada (115) y una porción del área segura aislada (115).

12. Un sistema implementado por ordenador para autenticar a un usuario, comprendiendo el sistema:

un procesador (114);

un área segura aislada (115), asociada con el procesador (114);

un medio no transitorio legible por ordenador (112), conectado operativamente al procesador (114);

una pantalla de visualización (130), conectada operativamente a un controlador de pantalla de visualización (142);

el controlador de la pantalla de visualización (142), conectado operativamente al procesador (114);

una pantalla táctil (134), conectada operativamente a un controlador de pantalla táctil (144);

el controlador de la pantalla táctil (144), conectado operativamente al procesador (114);

un elemento seguro (152), asociado con el procesador (114);

estando configurado el procesador (114) para causar:

generar una tabla de correspondencia, una distribución de los puntos de conexión y una representación visual de un teclado aleatorizado, asociando la tabla de correspondencia las posiciones de las teclas en el teclado aleatorizado y los valores, definiendo la distribución de los puntos de conexión geometrías y ubicaciones de las posiciones de las teclas en el teclado aleatorizado para ser pulsadas en la pantalla táctil (134), comprendiendo la representación visual del teclado aleatorizado los valores; transmitir, al elemento (152), la tabla de correspondencia;

transmitir, al controlador de pantalla (142), la representación visual del teclado aleatorizado;

transmitir, al controlador de la pantalla táctil (144), la distribución de los puntos de conexión;

causar la visualización, mediante el controlador la pantalla (142), del teclado aleatorizado en la pantalla (130);

detectar, mediante el controlador de la pantalla táctil (144), una entrada de evento táctil del usuario en la pantalla táctil (134);

generar, mediante el controlador de la pantalla táctil (144), un evento de codificación en base a la entrada del evento táctil y a la distribución de los puntos de conexión, identificando el evento de codificación la tecla correspondiente en el teclado aleatorizado pulsado por el usuario en la pantalla táctil (134);

encriptar, mediante el controlador de la pantalla táctil (144), el evento de codificación;

transmitir, al elemento seguro (152), el evento de codificación encriptado;

desencriptar, mediante el elemento seguro (152), el evento de codificación encriptado; y

reconstituir, mediante el elemento seguro (152), un código de identificación personal (PIC) asociado con el usuario en base al evento de codificación y a la tabla de correspondencia, recuperando el valor de la tabla de correspondencia correspondiente al evento de codificación.

13. El sistema de la reivindicación 12, en el que el área segura aislada (115) está alojada en un segundo procesador, diferente del procesador (114).

14. El sistema de cualquiera de las reivindicaciones 12 y 13, en el que el elemento seguro (152) es, al menos, uno de un elemento de hardware conectado operativamente al procesador (114), un componente de software ejecutado por el procesador (114), el área segura aislada (115) y una parte del área segura aislada (115).

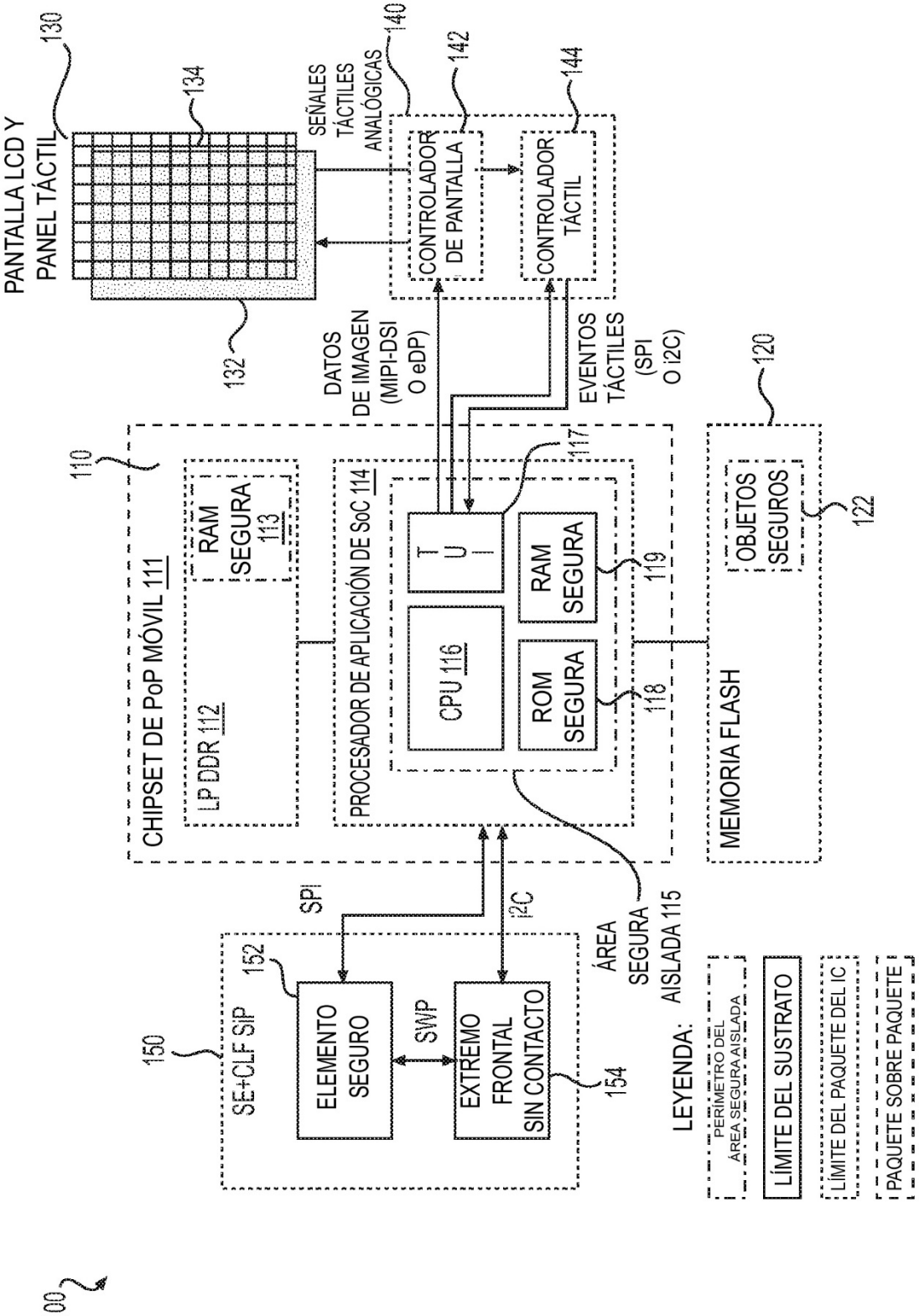
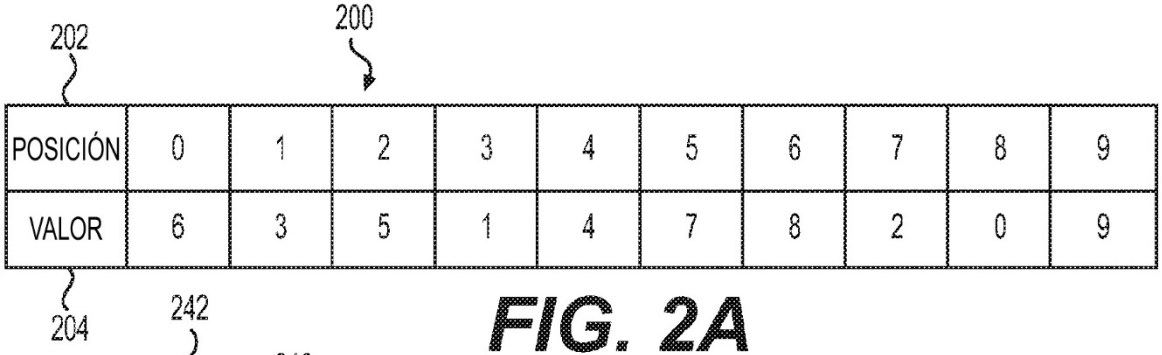
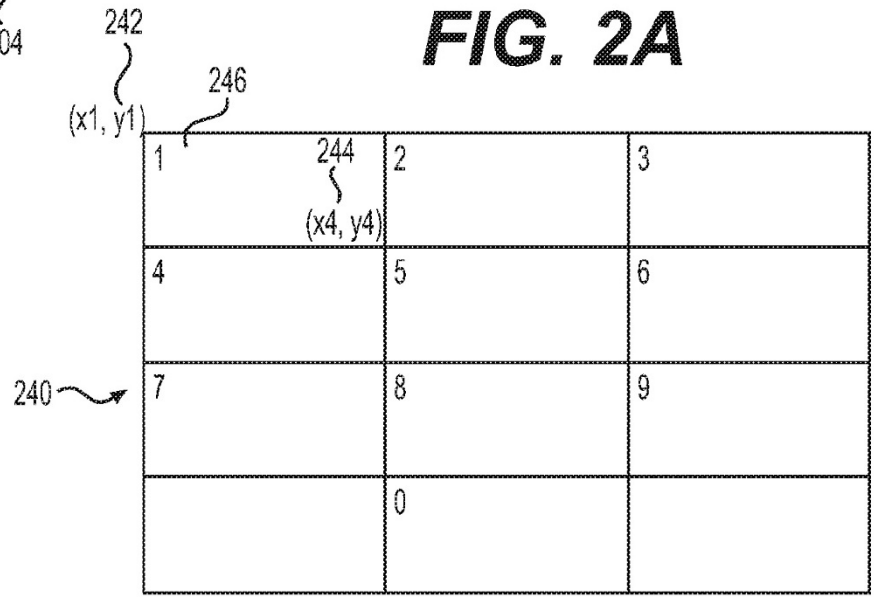

100
PANTALLA LCD Y PANEL TÁCTIL
130
134
132
SEÑALES TÁCTILES ANALÓGICAS
140
142
144
CONTROLADOR DE PANTALLA
CONTROLADOR TÁCTIL
DATOS DE IMAGEN (MIPI-DSI O eDP)
EVENTOS TÁCTILES (SPI O I2C)
110
CHIPSET DE PoP MÓVIL 111
LP DDR 112
RAM SEGURA 113
PROCESADOR DE APLICACIÓN DE SoC 114
CPU 116
T U I
117
RAM SEGURA
119
ROM SEGURA
118
120
MEMORIA FLASH
OBJETOS SEGUROS
122
SPI
I2C
ÁREA SEGURA AISLADA 115
150
SE+CLF SiP
152
ELEMENTO SEGURO
SWP
EXTREMO FRONTAL SIN CONTACTO
154
LEYENDA:
PERÍMETRO DEL ÁREA SEGURA AISLADA
LÍMITE DEL SUSTRATO
LÍMITE DEL PAQUETE DEL IC
PAQUETE SOBRE PAQUETE

FIG. 1



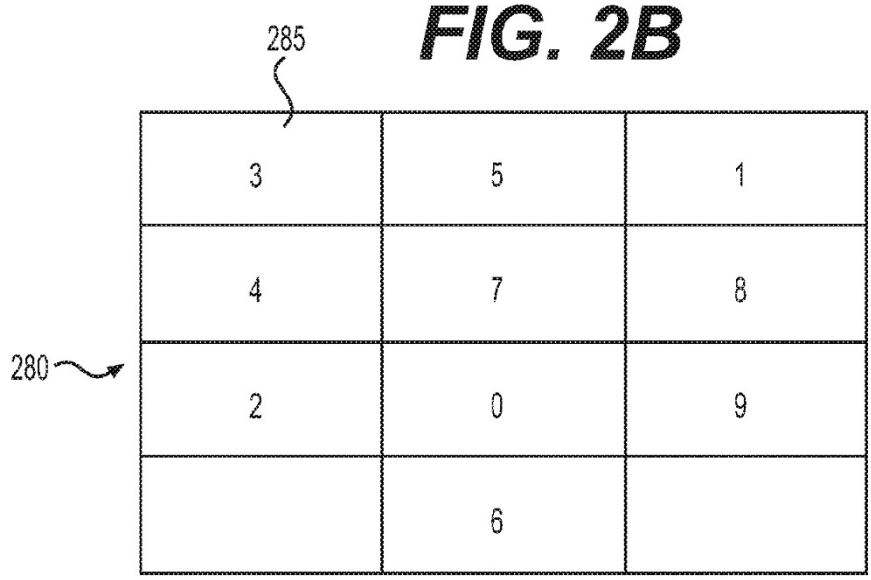
POSICIÓN	0	1	2	3	4	5	6	7	8	9
VALOR	6	3	5	1	4	7	8	2	0	9

FIG. 2A



1	2	3
4	5	6
7	8	9
	0	

FIG. 2B



3	5	1
4	7	8
2	0	9
	6	

FIG. 2C

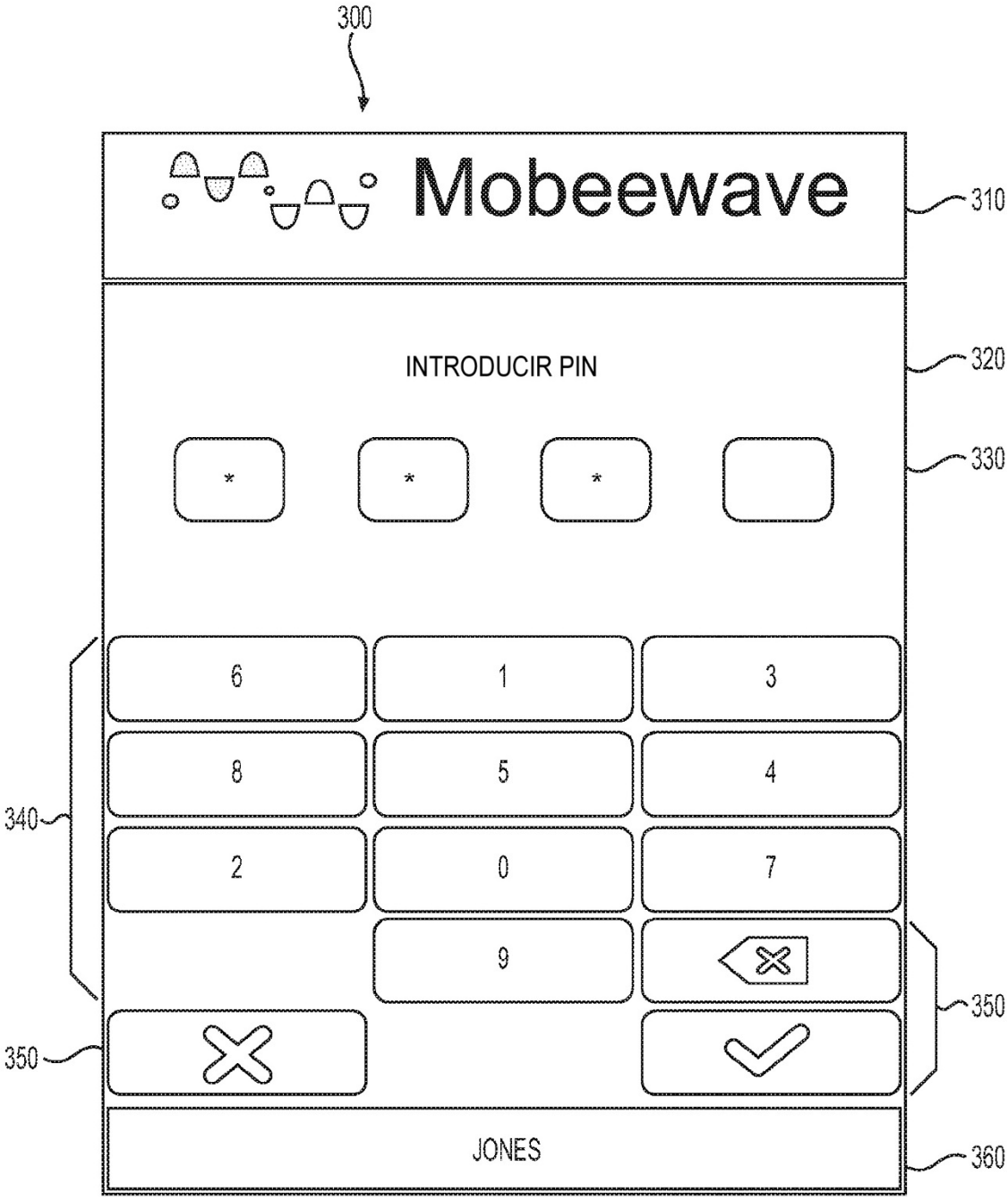

300
Mobeewave
310
INTRODUCIR PIN
320
*
*
*
330
6
1
3
8
5
4
340
2
0
7
9
350
350
JONES
360

FIG. 3

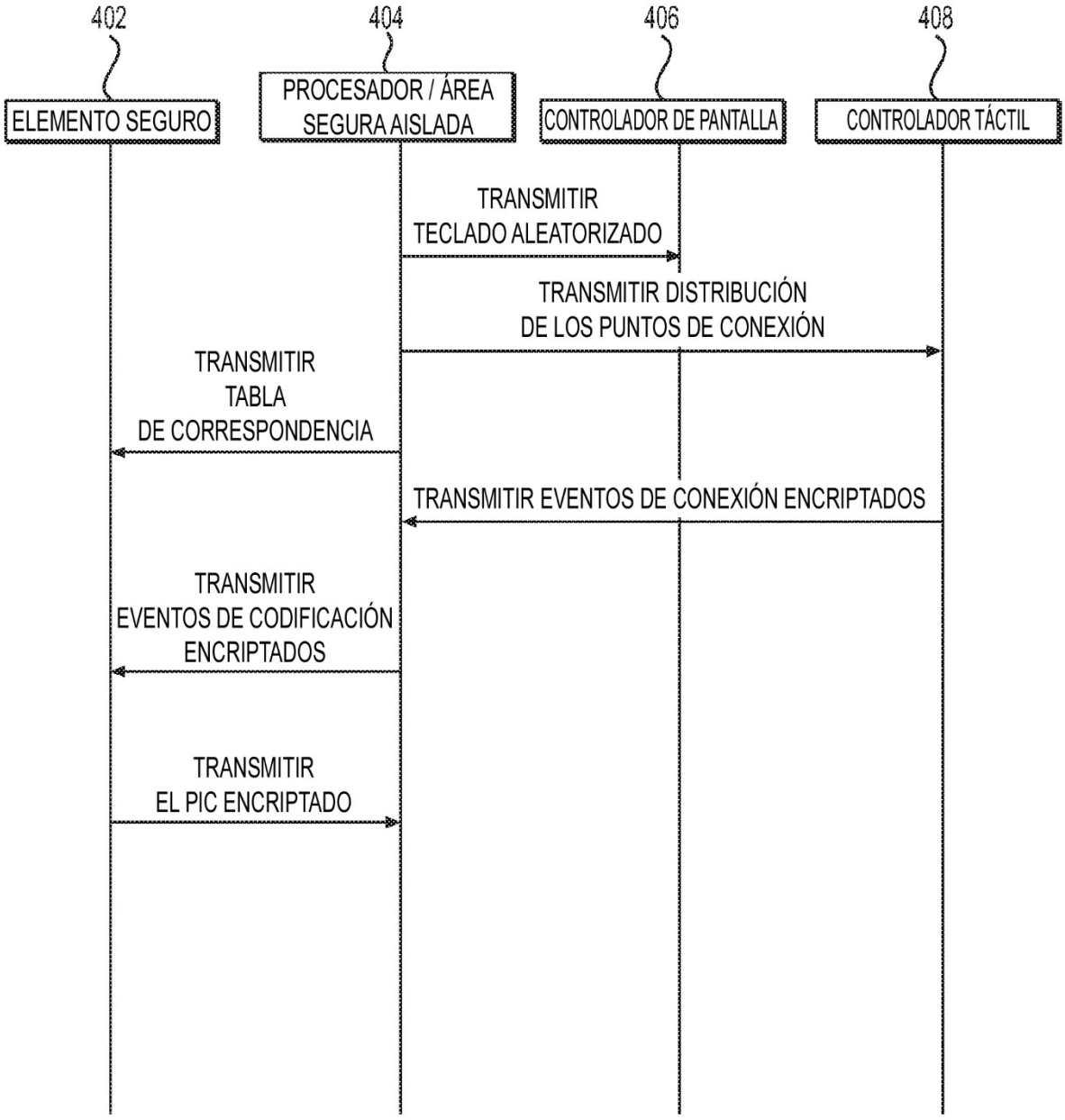

402
404
406
408
ELEMENTO SEGURO
PROCESADOR / ÁREA SEGURA AISLADA
CONTROLADOR DE PANTALLA
CONTROLADOR TÁCTIL
TRANSMITIR TECLADO ALEATORIZADO
TRANSMITIR DISTRIBUCIÓN DE LOS PUNTOS DE CONEXIÓN
TRANSMITIR TABLA DE CORRESPONDENCIA
TRANSMITIR EVENTOS DE CONEXIÓN ENCRIPTADOS
TRANSMITIR EVENTOS DE CODIFICACIÓN ENCRIPTADOS
TRANSMITIR EL PIC ENCRIPTADO

FIG. 4

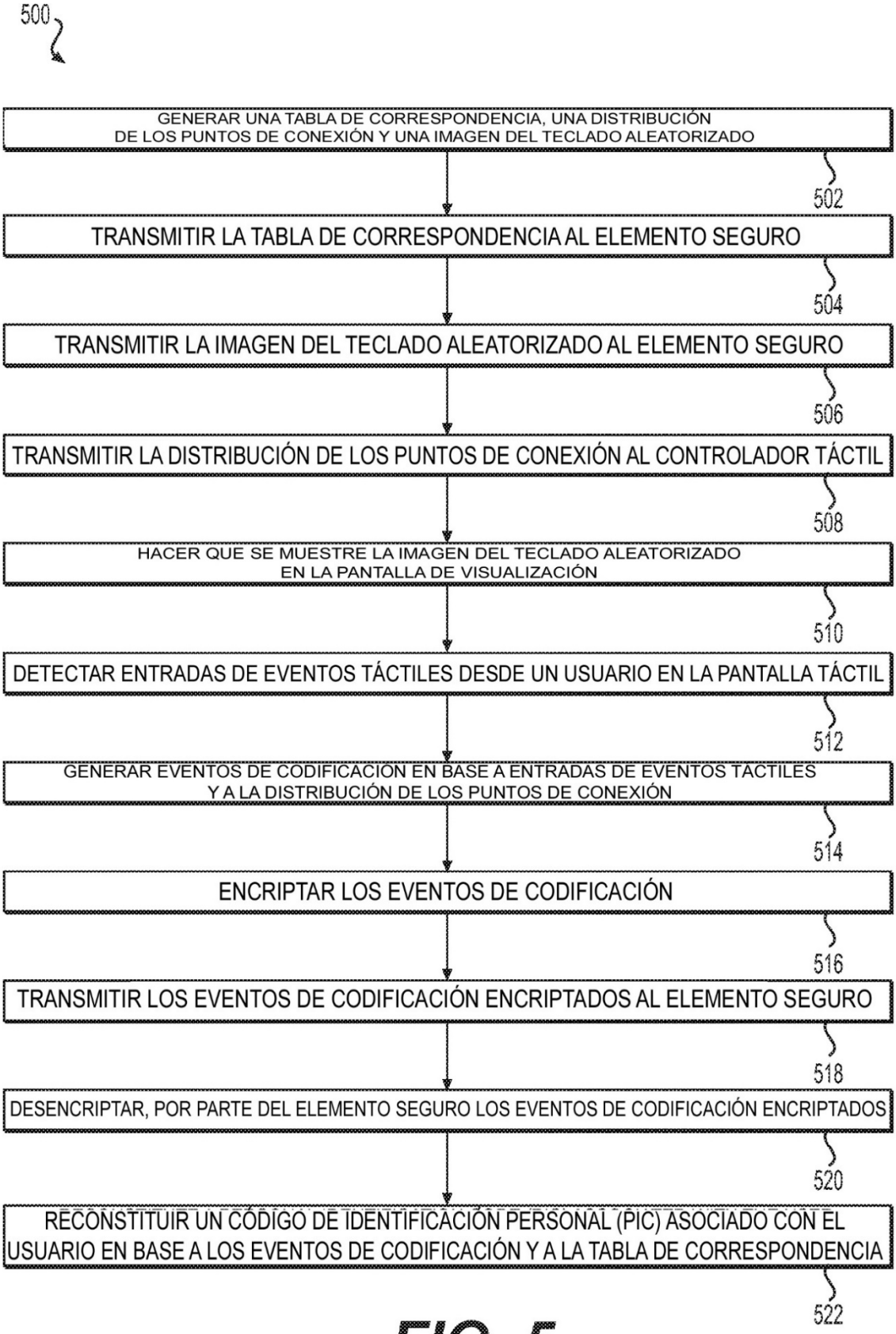

500
GENERAR UNA TABLA DE CORRESPONDENCIA, UNA DISTRIBUCIÓN DE LOS PUNTOS DE CONEXIÓN Y UNA IMAGEN DEL TECLADO ALEATORIZADO
502
TRANSMITIR LA TABLA DE CORRESPONDENCIA AL ELEMENTO SEGURO
504
TRANSMITIR LA IMAGEN DEL TECLADO ALEATORIZADO AL ELEMENTO SEGURO
506
TRANSMITIR LA DISTRIBUCIÓN DE LOS PUNTOS DE CONEXIÓN AL CONTROLADOR TÁCTIL
508
HACER QUE SE MUESTRE LA IMAGEN DEL TECLADO ALEATORIZADO EN LA PANTALLA DE VISUALIZACIÓN
510
DETECTAR ENTRADAS DE EVENTOS TÁCTILES DESDE UN USUARIO EN LA PANTALLA TÁCTIL
512
GENERAR EVENTOS DE CODIFICACIÓN EN BASE A ENTRADAS DE EVENTOS TÁCTILES Y A LA DISTRIBUCIÓN DE LOS PUNTOS DE CONEXIÓN
514
ENCRIPTAR LOS EVENTOS DE CODIFICACIÓN
516
TRANSMITIR LOS EVENTOS DE CODIFICACIÓN ENCRIPTADOS AL ELEMENTO SEGURO
518
DESENCRIPTAR, POR PARTE DEL ELEMENTO SEGURO LOS EVENTOS DE CODIFICACIÓN ENCRIPTADOS
520
RECONSTITUIR UN CÓDIGO DE IDENTIFICACIÓN PERSONAL (PIC) ASOCIADO CON EL USUARIO EN BASE A LOS EVENTOS DE CODIFICACIÓN Y A LA TABLA DE CORRESPONDENCIA
522

FIG. 5