(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 749 678**

(51) Int. CI.:

G06K 19/07 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **12.10.2015 PCT/EP2015/073545**

(87) Fecha y número de publicación internacional: **14.04.2016 WO16055663**

(96) Fecha de presentación y número de la solicitud europea: **12.10.2015 E 15778668 (2)**

(97) Fecha y número de publicación de la concesión europea: **17.07.2019 EP 3215984**

(54) Título: **Recolección de energía en un dispositivo RFID pasivo**

(30) Prioridad:

10.10.2014 US 201462062243 P
14.05.2015 GB 201508281

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
23.03.2020

(73) Titular/es:

ZWIPE AS (100.0%)
Rådhusgata 24
0151 Oslo , NO

(72) Inventor/es:

WENDLING, JEAN-HUGUES

(74) Agente/Representante:

ISERN JARA, Jorge

DESCRIPCIÓN

Recolección de energía en un dispositivo RFID pasivo

La presente invención se refiere a la recolección de energía en un dispositivo RFID, y particularmente a la recolección de energía en un dispositivo RFID pasivo que incluye componentes adicionales que requieren energía tal como un escáner de huellas dactilares.

La Figura 1 muestra la arquitectura de un dispositivo 2 RFID pasivo típico. Un lector 4 RFID energizado que transmite una señal a través de una antena 6. La señal es típicamente 13.56 MHz para los sistemas MIFARE® y DESFire®, fabricados por NXP Semiconductors, pero puede ser de 125 kHz para productos PROX® de baja frecuencia, fabricados por HID Global Corp. Esta señal es recibida por una antena 8 del dispositivo 2 RFID, que comprende una bobina y un condensador sintonizados, y luego pasa a un chip 10 RFID. La señal recibida es rectificada por un puente rectificador 12, y la salida de DC del rectificador 12 se proporciona a un circuito 14 de control que controla la mensajería desde el chip 10.

La salida de datos del circuito 14 de control está conectada a un transistor 16 de efecto de campo que está conectado a través de la antena 8. Al encender y apagar el transistor 16, el dispositivo 2 RFID puede transmitir una señal y decodificarla mediante circuitos 18 de control adecuados en el lector 4. Este tipo de señalización se conoce como modulación de retrodispersión y se caracteriza por el hecho de que el lector 4 se utiliza para alimentar el mensaje de retorno a sí mismo.

Como medida de seguridad adicional, algunos dispositivos RFID se han adaptado para procesar adicionalmente datos de identificación biométrica para proporcionar una seguridad mejorada. En tales sistemas, el usuario recibe una tarjeta RFID que tiene una plantilla biométrica almacenada en ella. Un terminal, por ejemplo, para permitir que el propietario de la tarjeta tenga acceso a dinero o acceso físico a un edificio u oficina, cuenta con un sensor de huellas dactilares y, para autorizar al usuario, se transmite una lectura de huella dactilar desde el terminal a la tarjeta RFID, donde se realiza una coincidencia con la plantilla almacenada en la tarjeta. La tarjeta RFID luego comunica de forma inalámbrica al terminal los resultados de la coincidencia en vivo, sí o no.

Se ha propuesto incorporar un sensor biométrico, como un escáner de huellas dactilares, en un dispositivo RFID pasivo. En el documento US 2013/207786 se divulga un dispositivo RFID de ejemplo que incorpora un sensor biométrico. Al menos las realizaciones preferidas de la presente invención buscan resolver algunos de los problemas técnicos asociados con dicho dispositivo.

La presente invención proporciona un método para recolectar energía en un dispositivo RFID pasivo que comprende un motor de autenticación biométrica pasiva, comprendiendo el método: recibir, mediante el dispositivo RFID, un comando de un lector RFID con alimentación; recibir, por el dispositivo RFID, un campo de excitación de radiofrecuencia continua sin pulsos mientras el lector RFID espera una respuesta al comando; recolecciona, mediante el dispositivo RFID, energía del campo de excitación; suministrar la energía extraída del campo de excitación al motor de autenticación biométrica; realizar un proceso en el motor de autenticación biométrica, el proceso no es necesario para responder al comando del lector RFID; determinar un período en el que el dispositivo RFID ha estado esperando una respuesta; y en respuesta a determinar que el período excede un umbral predeterminado si el proceso no se ha completado, enviar, mediante el dispositivo RFID, una solicitud de extensión del tiempo de espera al lector RFID.

Como se discutirá con mayor detalle a continuación, los lectores RFID típicos activan y desactivan su señal de excitación para conservar energía, en lugar de emitir constantemente la señal de excitación. A menudo, esta pulsación da como resultado un ciclo de trabajo de energía útil de menos del 10% de la energía emitida por una emisión constante. Esto puede ser insuficiente para energizar un motor de autenticación biométrica.

El método anterior supera este problema aprovechando ciertos aspectos de la funcionalidad estándar de un lector RFID que cumple, por ejemplo, con el estándar internacional ISO/IEC 14443. Particularmente, mientras el lector RFID espera una respuesta a un comando, debe mantener un campo de excitación de radiofrecuencia (RF) sin pulsos, preferiblemente sustancialmente continuo.

Por lo tanto, de conformidad con este método, cuando el lector RFID envía un comando al dispositivo RFID, el dispositivo no responde, sino que espera y recoge la energía para accionar la funcionalidad del motor de autenticación biométrica.

El proceso realizado por el motor de autenticación biométrica no es necesario para responder al comando, por ejemplo, el comando puede ser un comando de "solicitud para proporcionar código de identificación". Es decir, una respuesta al comando del dispositivo RFID se retrasa intencionalmente para permitir que se realice el procesamiento.

En las realizaciones preferidas, el dispositivo RFID no responde al comando mientras el motor de autenticación biométrica está realizando un proceso. Además, el método preferiblemente comprende, además: después de que el motor de autenticación biométrica completa el proceso, respondiendo mediante el dispositivo RFID al comando.

Los pasos de "determinar un período en el que el dispositivo RFID ha estado esperando una respuesta; y responder a la determinación de que el período excede un umbral predeterminado si el proceso no se ha completado, enviar mediante el dispositivo RFID una solicitud de extensión de tiempo de espera al lector RFID" se repite preferiblemente hasta que se complete el proceso y/o se haya enviado una respuesta al comando. Por ejemplo, después de que se haya completado el proceso, el dispositivo RFID puede permitir que expire el tiempo de espera, si no se requiere más comunicación con el lector RFID. Alternativamente, se puede enviar una respuesta al lector RFID, por ejemplo, si el proceso fue parte de un paso de autorización antes de responder al comando.

Preferiblemente, el período es un tiempo desde que se recibió el comando o desde que se realizó la última solicitud de extensión de tiempo de espera. Por lo tanto, la solicitud de una extensión del tiempo de espera se puede enviar antes de que expire el tiempo de espera actual para garantizar que el lector RFID continúe manteniendo el campo de excitación RF hasta que se complete el proceso.

El proceso realizado por el motor de autenticación biométrica puede ser uno de un proceso de inscripción biométrica o un proceso de coincidencia biométrica. El método descrito es particularmente aplicable a la coincidencia o inscripción biométrica, por ejemplo, a la coincidencia de huellas dactilares o a los procesos de inscripción, ya que estos procesos requieren la entrada del usuario (es decir, uno o más escaneos biométricos), que solo pueden procesarse a la velocidad que son suministrados por el usuario del dispositivo RFID.

Sin utilizar una solicitud de extensión de tiempo de espera, el tiempo predeterminado máximo que podría suministrar un campo de excitación RF sin pulsos es de 4.949 segundos para un lector de RFID que cumpla con el estándar internacional ISO/IEC 14443. Por lo tanto, el método permite procesos a realizar por el motor de autenticación biométrica, en donde el proceso requiere más de 5.0 segundos para completarse.

En diversas realizaciones, el motor de autenticación biométrica puede incluir un escáner biométrico y una unidad de procesamiento. Preferiblemente, el motor de autenticación biométrica es un motor de autenticación de huellas dactilares.

Como se discutió anteriormente, el presente método es particularmente aplicable a dispositivos y lectores que cumplen con el estándar internacional ISO/IEC 14443 (aunque el método puede ser aplicable también a otros estándares que funcionan de manera similar), y por lo tanto el dispositivo RFID es preferiblemente una tarjeta (PICC) de circuito integrado de proximidad y el lector RFID es preferiblemente un dispositivo (PCD) de acoplamiento de proximidad. El PICC y PCD cumplen preferiblemente con las definiciones establecidas en el estándar internacional ISO/IEC 14443.

El umbral predeterminado está preferiblemente por debajo de un primer tiempo de espera preestablecido del PICC y el PCD.

Vista desde un segundo aspecto, la presente invención proporciona un dispositivo RFID pasivo que comprende: una antena para recibir un campo de excitación de radiofrecuencia desde un lector RFID y para recolectar energía del campo de excitación; un motor de autenticación biométrica pasiva dispuesto para recibir energía recolectada por la antena; y un controlador de dispositivo RFID dispuesto para realizar un método, que comprende: recibir, por la antena, un comando de un lector RFID energizado; recibir, por la antena, un campo de excitación de radiofrecuencia sustancialmente continuo mientras el lector RFID espera una respuesta al comando; realizar un proceso en el motor de autenticación biométrica, el proceso no es necesario para responder al comando del lector RFID; determinar un período que el dispositivo RFID ha estado esperando una respuesta; y en respuesta a determinar que el período excede un umbral predeterminado si el proceso no se ha completado, enviando por la antena una solicitud de extensión del tiempo de espera al lector RFID.

El controlador del dispositivo RFID está preferiblemente dispuesto adicionalmente para realizar cualquiera o todos los pasos preferidos del método del primer aspecto.

El dispositivo RFID puede ser uno cualquiera de: una tarjeta de acceso, una tarjeta de crédito, una tarjeta de débito, una tarjeta prepaga, una tarjeta de fidelidad, una tarjeta de identidad, una tarjeta criptográfica o similares.

Algunas realizaciones preferidas de la presente invención se describirán ahora con mayor detalle, solo a modo de ejemplo y con referencia a las Figuras adjuntas, en las que:

La Figura 1 ilustra un circuito para un dispositivo RFID pasivo de la técnica anterior;

La Figura 2 ilustra un circuito para un dispositivo RFID pasivo que incorpora un escáner de huellas dactilares; y

La Figura 3 ilustra una carcasa externa para el dispositivo RFID pasivo que incorpora el escáner de huellas dactilares.

La Figura 2 muestra la arquitectura de un lector 104 RFID y un dispositivo 102 RFID pasivo, que es una variación del dispositivo 2 de RFID pasivo de la técnica anterior mostrado en la Figura 1. El dispositivo 102 RFID mostrado en la Figura 2 se ha adaptado para incluir un motor 120 de autenticación de huellas dactilares.

El lector 104 RFID es un lector de RFID convencional y está configurado para generar un campo de excitación RF usando una antena 106 de lector. La antena 106 de lector recibe además señales de RF entrantes del dispositivo 102 RFID, que son decodificadas por los circuitos 118 de control dentro del lector 104 RFID.

El dispositivo 102 RFID comprende una antena 108 para recibir una señal de RF (radiofrecuencia), un chip 110 RFID pasivo energizado por la antena y un motor 120 de autenticación de huellas dactilares pasivo energizado por la antena 108.

Como se usa en el presente documento, el término "dispositivo RFID pasivo" debe entenderse que significa un dispositivo 102 RFID en el que el chip 110 RFID es energizado solo por energía recolectada de un campo de excitación RF, por ejemplo, generada por el lector 118 RFID. Es decir, un dispositivo 102 RFID pasivo se basa en el lector 118 RFID para suministrar su energía para la transmisión. Un dispositivo 102 RFID pasivo normalmente no incluiría una batería, aunque se puede incluir una batería para energizar los componentes auxiliares del circuito (pero no para transmitir); dichos dispositivos a menudo se denominan "dispositivos RFID semi-pasivos".

De manera similar, el término "motor pasivo de huellas dactilares/autenticación biométrica" debe entenderse que significa un motor de autenticación biométrica/huellas dactilares que es alimentado solo con energía recolectada de un campo de excitación RF, por ejemplo, un campo de excitación RF generado por el lector 118 RFID)

La antena comprende un circuito sintonizado, en esta disposición incluye una bobina de inducción y un condensador, sintonizado para recibir una señal de RF del lector 104 RFID. Cuando se expone al campo de excitación generado por el lector 104 RFID, se induce un voltaje a través de la antena 108.

La antena 108 tiene líneas 122, 124 de salida de primer y segundo extremo, una en cada extremo de la antena 108. Las líneas de salida de la antena 108 están conectadas al motor 120 de autenticación de huellas dactilares para proporcionar energía al motor 120 de autenticación de huellas dactilares En esta disposición, se proporciona un rectificador 126 para rectificar el voltaje de AC recibido por la antena 108. El voltaje de DC rectificado se suaviza usando un condensador de suavizado y se suministra al motor 120 de autenticación de huellas dactilares.

El motor 120 de autenticación de huellas dactilares incluye una unidad 128 de procesamiento y un lector 130 de huellas dactilares, que es preferiblemente un lector 130 de huellas dactilares de área como se muestra en la figura 3. El motor 120 de autenticación de huellas dactilares es pasivo y, por lo tanto, es energizado solo por la salida de voltaje desde la antena 108. La unidad 128 de procesamiento comprende un microprocesador que se elige por ser de muy baja energía y muy alta velocidad, de modo que pueda realizar una compatibilidad biométrica en un tiempo razonable.

El motor 120 de autenticación de huellas dactilares está dispuesto para escanear un dedo o pulgar presentado al lector 130 de huellas dactilares y comparar la huella dactilar escaneada del dedo o pulgar con los datos de huellas dactilares previamente almacenados usando la unidad 128 de procesamiento. Luego se toma una determinación en cuanto a si la huella dactilar escaneada coincide con los datos de huella dactilar almacenados previamente. En una realización preferida, el tiempo requerido para capturar una imagen de huella dactilar y reconocer con precisión un dedo registrado es inferior a un segundo.

Si se determina una coincidencia, entonces el chip 110 RFID está autorizado para transmitir una señal al lector 104 RFID. En la disposición de la figura 2, esto se logra cerrando un interruptor 132 para conectar el chip 110 RFID a la antena 108. El chip 110 RFID es convencional y funciona de la misma manera que el chip 110 RFID mostrado en la figura 1 para transmitir una señal a través de la antena 108 usando modulación de retrodispersión activando y desactivando un transistor 116.

La figura 3 muestra una carcasa 134 de ejemplo del dispositivo 102 RFID. El circuito que se muestra en la figura 2 está alojado dentro de la carcasa 134 de tal manera que un área de escaneo del lector 130 de huellas dactilares queda expuesta desde la carcasa 134.

Antes de usar, el usuario del dispositivo 102 RFID debe primero registrar su fecha de huella dactilar en un dispositivo "virgen", es decir, sin incluir ningún dato biométrico pre-almacenado. Esto puede hacerse presentando su dedo al lector 130 de huellas dactilares una o más veces, preferiblemente al menos tres veces y usualmente de cinco a siete veces. En el documento WO 2014/068090 A1 se divulga un método de ejemplo de inscripción para una huella dactilar usando un sensor de tipo desplazamiento de baja energía, que los expertos en la materia podrán adaptar al sensor 130 de huella dactilar de área descrito aquí.

La carcasa puede incluir indicadores para la comunicación con el usuario del dispositivo RFID, tales como los LEDs 136, 138 mostrados en la figura 3. Durante la inscripción, el usuario puede guiarse por los indicadores 136, 138, que le indican al usuario si la huella dactilar ha sido registrada correctamente. Los LED 136, 138 en el dispositivo 102 RFID pueden comunicarse con el usuario transmitiendo una secuencia de destellos consistentes con las instrucciones que el usuario ha recibido con el dispositivo 102 RFID.

Después de varias presentaciones, la huella dactilar habrá sido registrada y el dispositivo 102 puede responder para siempre solo a su usuario original.

Con la biometría de huellas dactilares, un problema común ha sido que es difícil obtener resultados repetibles cuando la inscripción inicial se lleva a cabo en un lugar, tal como un terminal de inscripción dedicado, y la inscripción posterior para la correspondencia se lleva a cabo en otro, tal como el terminal donde se requiere la coincidencia. Las características mecánicas de la carcasa alrededor de cada sensor de huellas dactilares deben diseñarse cuidadosamente para guiar el dedo de manera consistente cada vez que se lea. Si se escanea una huella dactilar con un número de terminales diferentes, cada uno de ellos ligeramente diferente, entonces pueden producirse errores en la lectura de la huella dactilar. Por el contrario, si cada vez se usa el mismo sensor de huellas dactilares, se reduce la probabilidad de que ocurran tales errores.

Como se describió anteriormente, el presente dispositivo 102 incluye un motor 120 de autenticación de huellas dactilares que tiene un sensor 130 de huellas dactilares a bordo, así como la capacidad de inscribir al usuario, y, por lo tanto, los escaneos de coincidencia e inscripción pueden realizarse usando el mismo sensor 130 de huellas dactilares. Como resultado, los errores de escaneo se pueden equilibrar porque, si un usuario tiende a presentar su dedo con un sesgo lateral durante la inscripción, es probable que también lo haga durante el emparejamiento.

Por lo tanto, el uso del mismo sensor 130 de huellas dactilares para todos los escaneos utilizados con el dispositivo 102 RFID reduce significativamente los errores en la inscripción y la correspondencia, y por lo tanto produce resultados más reproducibles.

En la presente disposición, la energía para el chip 110 RFID y el motor 120 de autenticación de huellas dactilares se recolecta del campo de excitación generado por el lector 104 RFID. Es decir, el dispositivo 102 RFID es un dispositivo RFID pasivo, y por lo tanto no tiene batería, sino que utiliza la energía recoleccionada del lector 104 de manera similar a un dispositivo 2 RFID básico.

La salida rectificada del segundo rectificador 126 de puente se usa para energizar el motor 120 de autenticación de huellas dactilares. Sin embargo, la energía requerida para esto es relativamente alta en comparación con la demanda de energía de los componentes de un dispositivo 2 RFID normal. Por esta razón, no ha sido posible incorporar previamente un lector 130 de huellas dactilares en un dispositivo 102 RFID pasivo. En la presente disposición se utilizan consideraciones de diseño especiales para energizar el lector 130 de huellas dactilares usando la energía recoleccionada del campo de excitación del lector 104 RFID.

Un problema que surge cuando se busca energizar el motor 120 de autenticación de huellas dactilares es que los lectores 104 RFID típicos activan y desactivan su señal de excitación para conservar energía, en lugar de emitir constantemente la señal de excitación. A menudo, esta pulsación da como resultado un ciclo de trabajo de energía útil de menos del 10% de la energía emitida por una emisión constante. Esto es insuficiente para energizar el motor 120 de autenticación de huellas dactilares.

Los lectores 104 RFID pueden cumplir con ISO/IEC 14443, el estándar internacional que define las tarjetas de proximidad utilizadas para la identificación, y los protocolos de transmisión para comunicarse con ellas. Cuando se comunica con tales dispositivos 104 RFID, el dispositivo 102 RFID puede aprovechar una cierta característica de estos protocolos, que se describirá a continuación, para cambiar la señal de excitación del lector 104 RFID a continua durante el tiempo suficiente para realizar los cálculos necesarios.

El estándar ISO/IEC 14443-4 define el protocolo de transmisión para tarjetas de proximidad. ISO/IEC 14443-4 dicta un intercambio inicial de información entre una tarjeta (PICC) de circuito integrado de proximidad, es decir, el dispositivo 102 RFID, y un dispositivo (PCD) de acoplamiento de proximidad, es decir, el lector 104 RFID, que se utiliza, en parte, para negociar un marco de tiempo (FWT) de espera. El FWT define el tiempo máximo para que PICC comience su respuesta después del final de un marco de transmisión PCD. El PICC se puede establecer en la fábrica para solicitar un FWT que varíe de 302 µs a 4.949 segundos.

ISO/IEC14443-4 dicta que, cuando el PCD envía un comando al PICC, tal como una solicitud para que el PICC proporcione un código de identificación, el PCD debe mantener un campo de RF y esperar al menos un período de tiempo FWT para una respuesta del PICC antes de que decida que se ha producido un tiempo de espera de respuesta. Si el PICC necesita más tiempo que FWT para procesar el comando recibido del PCD, entonces el PICC puede enviar una solicitud de una extensión (S (WTX)) de tiempo de espera al PCD, lo que hace que el

temporizador FWT se restablezca a su valor negociado completo. Luego, se requiere que el PCD espere otro período de tiempo FWT completo antes de declarar una condición de tiempo de espera.

Si se envía una extensión (S (WTX)) de tiempo de espera adicional al PCD antes de que expire el FWT de reinicio, entonces el temporizador de FWT se restablece nuevamente a su valor negociado completo y se requiere que el PCD espere otro período completo de tiempo FWT antes de declarar una condición de tiempo de espera.

Este método de enviar solicitudes para una extensión de tiempo de espera se puede usar para mantener el campo de RF encendido durante un período de tiempo indefinido. Mientras se mantiene este estado, el progreso de la comunicación entre el PCD y el PICC se detiene y el campo de RF se puede utilizar para recolectar energía para accionar otros procesos que normalmente no están asociados con la comunicación con tarjeta inteligente, tal como la inscripción o verificación de huellas dactilares.

Por lo tanto, con algunos mensajes cuidadosamente diseñados entre la tarjeta y el lector, se puede extraer suficiente energía del lector para permitir el ciclo de autenticación. Este método de recolección de energía supera uno de los principales problemas de energizar un motor 120 de autenticación pasiva de huellas dactilares en un dispositivo 102 RFID pasivo, particularmente para cuando se debe registrar una huella dactilar.

Además, este método de recolección de energía permite que se use un escáner 130 de huellas dactilares más grande, y particularmente un escáner 130 de huellas dactilares de área, que genera datos que son computacionalmente menos intensivos para procesar.

Como se discutió anteriormente, antes de usar el dispositivo 102 RFID, el usuario del dispositivo 102 primero debe inscribirse en el dispositivo 102 “virgen”. Después de la inscripción, el dispositivo 102 RFID responderá solo a este usuario. En consecuencia, es importante que solo el usuario previsto pueda registrar su huella dactilar en el dispositivo 102 RFID.

Una medida de seguridad típica para una persona que recibe una nueva tarjeta de crédito o chip por correo es enviar la tarjeta a través de un correo y otro PIN asociado con la tarjeta. Sin embargo, para un dispositivo 102 RFID autenticado biométricamente, tal como el descrito anteriormente, este proceso es más complicado. A continuación, se describe un método de ejemplo para garantizar que solo el destinatario previsto del dispositivo 102 RFID pueda registrar su huella dactilar.

Como se indicó anteriormente, el dispositivo 102 RFID y un PIN único asociado con el dispositivo 102 RFID se envían por separado al usuario. Sin embargo, el usuario no puede usar la funcionalidad de autenticación biométrica de la tarjeta 102 RFID hasta que haya registrado su huella dactilar en el dispositivo 102 RFID.

El usuario recibe instrucciones de ir a un terminal de punto de venta que está equipado para poder leer tarjetas sin contacto y presentar su dispositivo 102 RFID al terminal. Al mismo tiempo, ingresa su PIN en la terminal a través de su teclado.

El terminal enviará el PIN ingresado al dispositivo 102 RFID. Como la huella dactilar del usuario aún no se ha registrado en el dispositivo 102 RFID, el dispositivo 102 RFID comparará la entrada del teclado con el PIN del dispositivo 102 RFID. Si los dos son iguales, entonces la tarjeta se vuelve registrable.

El usuario de la tarjeta puede entonces registrar su huella dactilar usando el método descrito anteriormente. Alternativamente, si el usuario tiene una fuente de energía adecuada disponible en su hogar, puede llevar el dispositivo 102 RFID a su casa y pasar por un procedimiento de inscripción biométrica en un momento posterior.

El dispositivo 102 RFID, una vez inscrito, puede usarse sin contacto usando una huella dactilar, sin PIN, o solo con el PIN, dependiendo del monto de la transacción que tiene lugar.

REIVINDICACIONES

1. Un método para recolectar energía en un dispositivo (102) RFID pasivo que comprende un motor (120) de autenticación biométrica pasiva, comprendiendo el método:

recibir, por el dispositivo RFID, un comando de un lector (104) RFID energizado;

recibir, por el dispositivo RFID, un campo de excitación de radiofrecuencia continua sin pulsos mientras el lector RFID espera una respuesta al comando;

recolectar, mediante el dispositivo RFID, energía del campo de excitación;

suministrar la energía extraída del campo de excitación al motor de autenticación biométrica; realizar un proceso en el motor de autenticación biométrica, el proceso no es necesario para responder al comando del lector RFID;

determinar un período en el que el dispositivo RFID ha estado esperando una respuesta; y

en respuesta a la determinación de que el período excede un umbral predeterminado, si el proceso no se ha completado, enviar, mediante el dispositivo RFID, una solicitud de extensión del tiempo de espera al lector RFID.

2. Un método de acuerdo con la reivindicación 1, en donde el dispositivo RFID no responde al comando mientras el motor de autenticación biométrica está realizando el proceso.

3. Un método de acuerdo con la reivindicación 1 o 2, que comprende, además:

después de que el motor de autenticación biométrica completa el proceso, respondiendo mediante el dispositivo RFID al comando.

4. Un método de acuerdo con cualquier reivindicación precedente, en donde los pasos de determinar un período y enviar una solicitud de extensión de tiempo de espera al lector RFID se repiten hasta que se complete el proceso y/o se haya enviado una respuesta al comando.

5. Un método de acuerdo con cualquier reivindicación precedente, en donde el período es un tiempo desde que se recibió el comando o desde que se realizó la última solicitud de extensión de tiempo de espera.

6. Un método de acuerdo con cualquiera de las reivindicaciones anteriores, en donde el proceso realizado por el motor de autenticación biométrica es uno de un proceso de inscripción biométrica y un proceso de correspondencia biométrica, y/o en donde el proceso requiere más de 5.0 segundos para completarse.

7. Un método de acuerdo con cualquiera de las reivindicaciones anteriores, en donde el motor de autenticación biométrica incluye un escáner biométrico y una unidad de procesamiento, y preferiblemente en donde el motor de autenticación biométrica es un motor de autenticación de huellas dactilares y el escáner biométrico es un escáner de huellas dactilares.

8. Un dispositivo (102) RFID pasivo que comprende:

una antena (108) para recibir un campo de excitación de radiofrecuencia de un lector RFID y para recolectar energía del campo de excitación;

un motor (120) pasivo de autenticación biométrica dispuesto para recibir la energía recoleccionada por la antena; y

un controlador (128) de dispositivo RFID dispuesto para realizar un método, que comprende:

recibir, por la antena, un comando de un lector (104) RFID energizado;

recibir, por la antena, un campo de excitación de radiofrecuencia sustancialmente continuo mientras el lector RFID espera una respuesta al comando;

realizar un proceso en el motor de autenticación biométrica, el proceso no es necesario para responder al comando del lector RFID;

determinar un período en el que el dispositivo RFID ha estado esperando una respuesta; y

en respuesta a determinar que el período excede un umbral predeterminado si el proceso no se ha completado, enviando por la antena una solicitud de extensión del tiempo de espera al lector RFID.

9. Un dispositivo RFID pasivo de acuerdo con la reivindicación 8, en donde el controlador RFID está configurado para no responder al comando mientras el motor de autenticación biométrica está realizando un proceso.

10. Un dispositivo RFID pasivo de acuerdo con la reivindicación 8 o 9, en donde el método comprende, además: después de que el motor de autenticación biométrica completa el proceso, responder mediante el dispositivo RFID al comando.

11. Un dispositivo RFID pasivo de acuerdo con cualquiera de las reivindicaciones 8 a 10, en donde los pasos para determinar un período y enviar una solicitud de extensión del tiempo de espera al lector RFID se repiten hasta que se complete el proceso y/o una respuesta al comando ha sido enviada, y/o en donde el período es un tiempo desde que se recibió el comando o desde que se realizó la última solicitud de extensión de tiempo de espera.

12. Un dispositivo RFID pasivo de acuerdo con cualquiera de las reivindicaciones 8 a 11, en donde el proceso realizado por el motor de autenticación biométrica es uno de un proceso de inscripción biométrica y un proceso de correspondencia biométrica, y/o en donde el proceso requiere más de 5.0 segundos para ser terminado.

13. Un dispositivo RFID pasivo de acuerdo con cualquiera de las reivindicaciones 8 a 12, en donde el motor de autenticación biométrica incluye un escáner biométrico y una unidad de procesamiento, y preferiblemente en donde el motor de autenticación biométrica es un motor de autenticación de huellas dactilares y el escáner biométrico es un escáner de huellas dactilares.

14. Un método o un dispositivo RFID pasivo de acuerdo con cualquiera de las reivindicaciones anteriores, en donde el dispositivo RFID pasivo es una tarjeta (PICC) de circuito integrado de proximidad y el lector RFID es un dispositivo (PCD) de acoplamiento de proximidad.

15. Un método o un dispositivo RFID pasivo de acuerdo con cualquiera de las reivindicaciones anteriores, en donde el umbral predeterminado se establece en menos del primer tiempo de espera (FWT) del PCD.

Fig. 1

ESTADO DE LA TÉCNICA

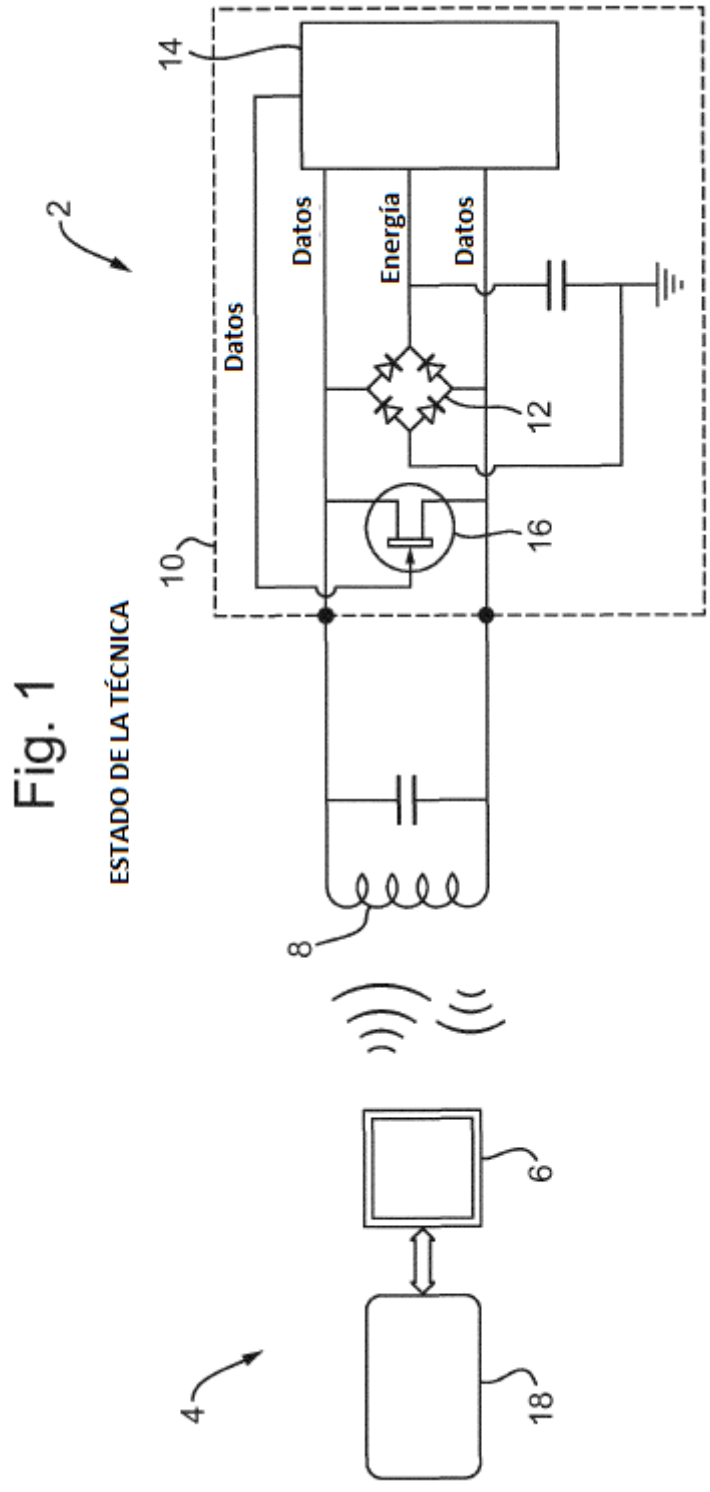

Fig. 2

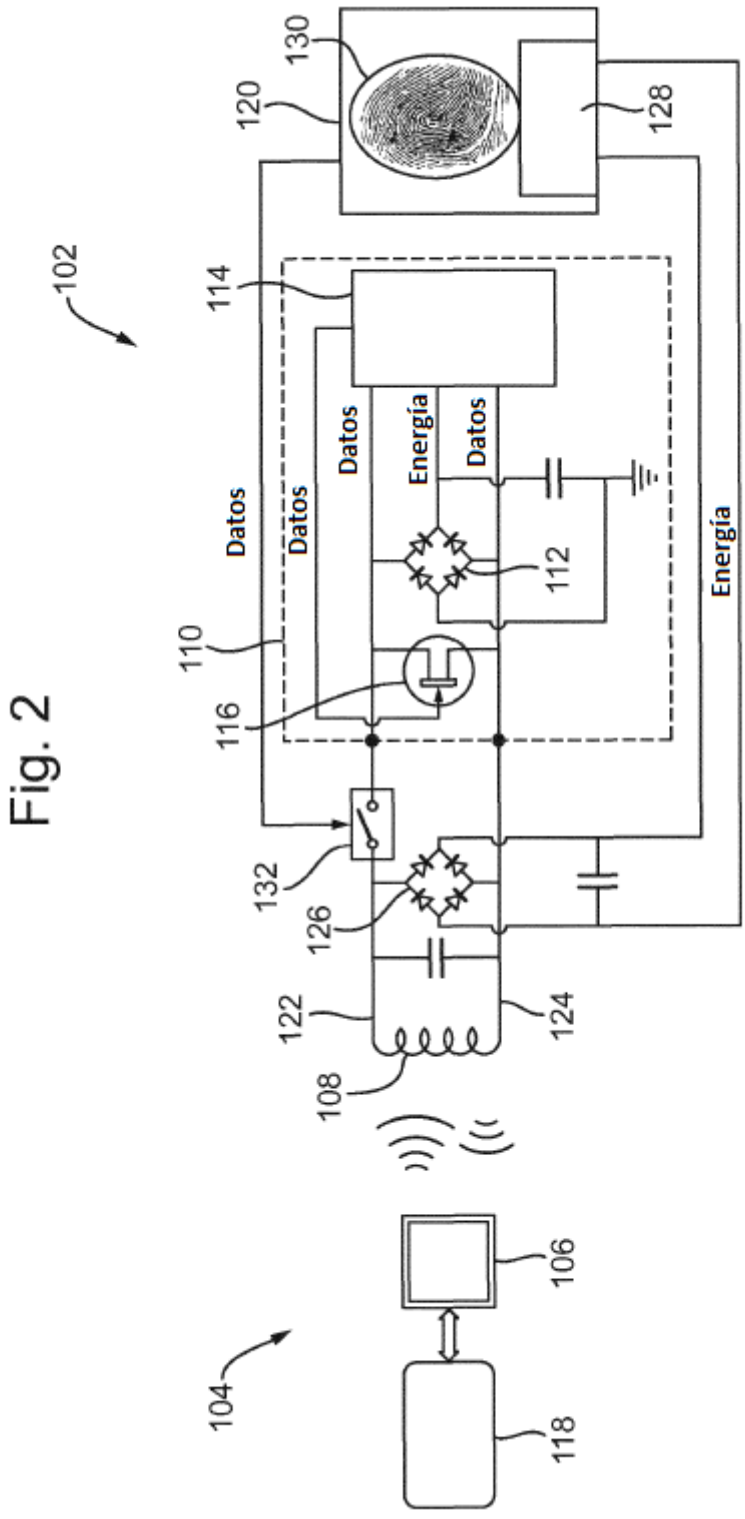
102
104
106
108
110
112
114
116
118
120
122
124
126
128
130
132
Datos
Datos
Datos
Energía
Datos
Energía

Fig. 3