(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 923 153**

(51) Int. CI.:

| | | | |
|---|---|---|---|
| ***A61B 5/00*** | (2006.01) | ***H04W 8/00*** | (2009.01) |
| ***A61B 5/083*** | (2006.01) | ***H04L 9/08*** | (2006.01) |
| ***A61M 5/172*** | (2006.01) | ***H04W 12/50*** | (2011.01) |
| ***H04W 4/80*** | (2008.01) | ***H04W 12/041*** | (2011.01) |
| ***H04W 76/10*** | (2008.01) | ***G16H 40/67*** | (2008.01) |
| ***A61B 5/145*** | (2006.01) | | |
| ***A61M 5/142*** | (2006.01) | | |
| ***H04W 12/00*** | (2011.01) | | |
| ***H04W 12/04*** | (2011.01) | | |
| ***H04W 84/18*** | (2009.01) | | |

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **21.05.2018 PCT/US2018/033614**

(87) Fecha y número de publicación internacional: **29.11.2018 WO18217605**

(96) Fecha de presentación y número de la solicitud europea: **21.05.2018 E 18806543 (7)**

(97) Fecha y número de publicación de la concesión europea: **29.06.2022 EP 3629897**

(54) Título: **Sistemas, aparatos y métodos de emparejamiento inalámbrico seguro entre dos dispositivos, que utiliza generación de claves fuera de banda (OOB) integrada**

(30) Prioridad:

**22.05.2017 US 201762509383 P**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
**23.09.2022**

(73) Titular/es:

**BECTON, DICKINSON AND COMPANY (100.0%)**
**1 Becton Drive**
**Franklin Lakes, NJ 07417-1880, US**

(72) Inventor/es:

**ZHENG, PING;**
**KASHEF, MOJTABA y**
**SU, YI**

(74) Agente/Representante:

**ELZABURU, S.L.P**

Aviso: En el plazo de nueve meses a contar desde la fecha de publicación en el Boletín Europeo de Patentes, de la mención de concesión de la patente europea, cualquier persona podrá oponerse ante la Oficina Europea de Patentes a la patente concedida. La oposición deberá formularse por escrito y estar motivada; sólo se considerará como formulada una vez que se haya realizado el pago de la tasa de oposición (art. 99.1 del Convenio sobre Concesión de Patentes Europeas).

## DESCRIPCIÓN

Sistemas, aparatos y métodos de emparejamiento inalámbrico seguro entre dos dispositivos, que utiliza generación de claves fuera de banda (OOB) integrada

Campo técnico:
La presente descripción se refiere a sistemas, métodos y aparatos de emparejamiento inalámbrico seguro entre dos dispositivos utilizando generación de claves fuera de banda (OOB) integrada, para minimizar el emparejamiento entre un dispositivo y un dispositivo no deseado y la interferencia maliciosa con un dispositivo emparejado.

Antecedentes:
La demanda de dispositivos médicos corporales (por ejemplo, bombas de infusión ponibles) y dispositivos médicos de red del área corporal (BAN) (por ejemplo, medidores portátiles de glucosa en sangre, teléfonos inteligentes con aplicaciones de tratamiento de afecciones médicas y controladores inalámbricos para dispositivos corporales) ha estado aumentando junto con un aumento en el deseo de los pacientes y los proveedores de atención médica de un tratamiento mejor y más cómodo de afecciones médicas como la diabetes.

El emparejamiento seguro entre dos dispositivos, tal como entre un dispositivo médico ponible y un controlador dedicado independiente o un teléfono inteligente con (por ejemplo, un teléfono inteligente con una aplicación relacionada con el funcionamiento del dispositivo médico ponible), es importante para evitar operaciones no deseadas o posibles interferencias maliciosas con las operaciones, del dispositivo médico. Además, también es importante evitar el emparejamiento del dispositivo médico con otro dispositivo no deseado, en particular cuando existen múltiples dispositivos potenciales con los que se puede emparejar un dispositivo médico dentro de la misma área.

La tecnología Bluetooth Smart o Bluetooth de baja energía (Bluetooth Low Energy, BLE) proporciona un protocolo efectivo de bajo consumo para conectar dispositivos de forma inalámbrica, incluidos dispositivos que funcionan con fuentes de alimentación, tales como baterías de tipo botón, como suele ser el caso de los dispositivos ponibles. Bluetooth Smart o BLE actualmente tiene tres opciones de emparejamiento, es decir, Entrada con clave de paso (Passkey Entry), Funciona directamente (Just Works) y OOB (Out-of-Band, fuera de banda), que pueden o no usarse con varios dispositivos dependiendo de diferentes factores, como las capacidades de entrada/salida de un dispositivo (IO) y el nivel de seguridad necesario para la aplicación o función de los dispositivos emparejados. Por ejemplo, los dispositivos BLE que no tienen capacidades de E/S física o capacidad de comunicación de campo cercano (NFC) no pueden usar el método de emparejamiento OOB porque el usuario tiene que introducir datos de autenticación OOB en los dispositivos homólogos. Por otro lado, ninguna de las opciones de emparejamiento Funciona directamente y emparejamiento de Entrada con clave de paso ha demostrado ser lo suficientemente segura para muchas aplicaciones inalámbricas, como aplicaciones médicas que requieren un alto nivel de seguridad y, por lo tanto, formas de emparejamiento más seguras.

En la patente US 2015/341785 A1, se da a conocer un sistema y un método para iniciar una sesión de comunicación bidireccional segura con un dispositivo médico implantable. El sistema y el método de la patente US 2015/341785 A1 incluyen configurar un dispositivo generador de pulsos (PG) y un dispositivo externo para establecer un enlace de comunicación entre ambos a través de un protocolo inalámbrico con un procedimiento de vinculación definido. El sistema y el método de la patente US 2015/341785 A1 también incluyen transmitir una identificación estática y una semilla dinámica desde el dispositivo PG a través de un canal de anuncio dedicado, al dispositivo externo y generar una clave de acceso a partir de un algoritmo predefinido en base a la semilla dinámica y una identificación estática. Además, el sistema y el método de la patente US 2015/341785 A1 incluyen iniciar el procedimiento de vinculación definido.

De acuerdo con la patente WO 2016/058965 A1, unas credenciales de un solo uso para un emparejamiento seguro automatizado de Bluetooth de varios dispositivos de comunicación pueden beneficiarse de credenciales de un solo uso aplicadas en un emparejamiento seguro automatizado, para mejorar la seguridad del emparejamiento. Por ejemplo, según la patente WO 2016/058965 A1, ciertos dispositivos de comunicación no atendidos capaces de implementar mecanismos utilizados para un emparejamiento por Bluetooth para autenticarse entre sí pueden beneficiarse de credenciales de un solo uso aplicadas en el emparejamiento seguro automatizado por Bluetooth. Un método puede incluir iniciar el emparejamiento por Bluetooth desde un primer dispositivo a un segundo dispositivo. El método, según la patente WO 2016/058965 A1, también puede incluir consultar al segundo dispositivo un valor secuencias antes de que se inicie el emparejamiento. El método de la patente WO 2016/058965 A1 puede incluir además calcular con un algoritmo arbitrario una clave de paso/número de identificación personal del primer dispositivo para el emparejamiento. El método de la patente WO 2016/058965 A1 también puede incluir el emparejamiento, con el número de identificación personal/clave de acceso, del primer dispositivo con el segundo dispositivo. En la patente WO 2016/058965 A1, el número de identificación personal/clave de paso se puede determinar en base a al menos un secreto compartido arbitrario entre el primer dispositivo y el segundo dispositivo, y el valor secuencial.

La patente EP 2 320 621 A1 y el documento de YAN MICHALEVSKY et al., "MASHaBLE", INFORMÁTICA MÓVIL Y REDES, ACM, 2 PENN PLAZA, SUITE 701 NUEVA YORK NY 10121-0701 EE. UU., (20161003), doi: 10.1145/2973750.2973778, ISBN 978-1-4503-4226-1, muestran el estado de la técnica relevante adicional.

COMPENDIO

Los objetivos de la invención se consiguen con un método según se define en la reivindicación 1 y con dispositivos según se define en las reivindicaciones 9 y 10.

Los problemas anteriores y otros se superan y se obtienen ventajas adicionales, mediante realizaciones ilustrativas de la presente invención. Las realizaciones ilustrativas dan a conocer un método de generación de claves OOB (por ejemplo, para usar con emparejamiento OOB) mediante el que los dispositivos a emparejar no requieren una funcionalidad IO para introducir datos de autenticación. Las realizaciones ilustrativas también dan a conocer un método de generación de claves OOB integrada, para emparejar de forma segura un dispositivo de administración de fármacos y/o corporal con dispositivos inalámbricos o móviles, por lo que el dispositivo de administración de fármacos y/o corporal no requiere una pantalla o un dispositivo de entrada clave para introducir datos de autenticación, simplificando así su diseño y reduciendo su coste.

Es un aspecto de las realizaciones ilustrativas de la presente invención dar a conocer un método de generación de claves para emparejar de forma segura un primer dispositivo con un segundo dispositivo para comunicación inalámbrica entre ambos, que comprende proporcionar a cada uno del primer dispositivo y el segundo dispositivo una credencial y una función resumen; transmitiendo el primer dispositivo señales de anuncio a intervalos seleccionados y en un rango de radiofrecuencia seleccionado a través de una primera antena; escaneando el segundo dispositivo la radiofrecuencia seleccionada a través de una segunda antena; proporcionando el primer dispositivo datos a compartir con el segundo dispositivo en las señales de anuncio; recibiendo el segundo dispositivo los datos compartidos a través del escaneo; y utilizando, cada uno del segundo dispositivo y el primer dispositivo, los datos compartidos y la credencial como entrada a la función resumen para generar una clave, siendo la clave generada por el primer dispositivo idéntica a la clave generada por el segundo dispositivo.

De acuerdo con aspectos de realizaciones ilustrativas de la presente invención, la provisión comprende preconfigurar el primer dispositivo y el segundo dispositivo con la credencial y la función resumen.

De acuerdo con aspectos de realizaciones ilustrativas de la presente invención, la credencial es una clave secreta predefinida de 128 bits.

De acuerdo con aspectos de realizaciones ilustrativas de la presente invención, las señales de anuncio se generan y transmiten de acuerdo con las especificaciones de Bluetooth de baja energía (BLE).

De acuerdo con aspectos de realizaciones ilustrativas de la presente invención, la función resumen es un algoritmo resumen seguro seleccionado del grupo que consiste en AES-128 o SHA-256.

De acuerdo con aspectos de realizaciones ilustrativas de la presente invención, los datos compartidos son únicos para el primer dispositivo y comprenden al menos una dirección de control de acceso al medio (MAC) y un parámetro único dinámico.

De acuerdo con aspectos de realizaciones ilustrativas de la presente invención, la clave es una clave fuera de banda (OOB) de 128 bits.

De acuerdo con aspectos de realizaciones ilustrativas de la presente invención, el rango de radiofrecuencia seleccionado puede ser un rango de 2,40-2,48 gigahercios (GHz).

Es un aspecto de las realizaciones ilustrativas de la presente invención dar a conocer un dispositivo para emparejamiento seguro con un segundo dispositivo para comunicación inalámbrica entre ambos, que comprende: un dispositivo de memoria configurado para almacenar una credencial y una función resumen; una interfaz de radiofrecuencia (RF) para transmitir y recibir señales de RF a través de al menos una antena; y un controlador. El controlador está configurado para transmitir señales de anuncio a intervalos seleccionados y en un rango de radiofrecuencia seleccionado a través de la interfaz RF y la antena. Las señales de anuncio comprenden datos a compartir con un segundo dispositivo. El controlador introduce los datos compartidos y la credencial en la función resumen para generar una clave. La clave generada por el dispositivo es idéntica a una clave generada por el segundo dispositivo cuando este busca y recibe del dispositivo las señales de anuncio con los datos compartidos.

Es un aspecto de las realizaciones ilustrativas de la presente invención dar a conocer un dispositivo para emparejamiento seguro con un segundo dispositivo para comunicación inalámbrica entre ambos, que comprende: un dispositivo de memoria configurado para almacenar una credencial y una función resumen; una interfaz de radiofrecuencia (RF) para transmitir y recibir señales de RF a través de al menos una antena; y un controlador. El controlador está configurado para buscar y recibir, a través de la interfaz de RF y la antena, señales de anuncio que son transmitidas por un segundo dispositivo a intervalos seleccionados y en un rango de radiofrecuencia

seleccionado. Las señales de anuncio comprenden datos del segundo dispositivo a compartir con el dispositivo. El controlador introduce los datos compartidos y la credencial en la función resumen para generar una clave. La clave generada por el dispositivo es idéntica a una clave generada por el segundo dispositivo.

De acuerdo con aspectos de realizaciones ilustrativas de la presente invención, el dispositivo y el segundo dispositivo están preconfigurados con la credencial y la función resumen.

De acuerdo con aspectos de realizaciones ilustrativas de la presente invención, la credencial es una clave secreta predefinida de 128 bits.

De acuerdo con aspectos de realizaciones ilustrativas de la presente invención, las señales de anuncio se generan y transmiten de acuerdo con las especificaciones de Bluetooth de baja energía (BLE).

De acuerdo con aspectos de realizaciones ilustrativas de la presente invención, la función resumen es un algoritmo resumen seguro seleccionado del grupo que consiste en AES-128 o SHA-256.

De acuerdo con aspectos de realizaciones ilustrativas de la presente invención, los datos compartidos son exclusivos de cualquiera del dispositivo y del segundo dispositivo que transmita las señales de anuncio. Los datos compartidos comprenden al menos una dirección de control de acceso al medio (MAC) y un parámetro único dinámico asociado con el correspondiente del dispositivo y el segundo dispositivo que transmita las señales de anuncio.

De acuerdo con aspectos de realizaciones ilustrativas de la presente invención, la clave es una clave fuera de banda (OOB) de 128 bits.

Los aspectos y ventajas adicionales y/u otros, de las realizaciones ilustrativas de la presente invención, se expondrán en la siguiente descripción, o serán evidentes a partir de la descripción, o pueden aprenderse mediante la práctica de realizaciones ilustrativas de la presente invención. Las realizaciones ilustrativas de la presente invención pueden comprender dispositivos a emparejar y métodos para hacer funcionar los mismos que tengan uno o más de los aspectos anteriores, y/o una o más de las características y combinaciones de los mismos. Las realizaciones ilustrativas de la presente invención pueden comprender una o más de las características y/o combinaciones de los aspectos anteriores como se indica, por ejemplo, en las reivindicaciones adjuntas.

BREVE DESCRIPCIÓN DE LOS DIBUJOS

Los aspectos anteriores y/u otros. y las ventajas de las realizaciones de la invención se apreciarán más fácilmente a partir de la siguiente descripción detallada, tomada junto con los dibujos adjuntos, de los que:

La figura 1 representa un dispositivo médico y un controlador de acuerdo con una realización ilustrativa de la presente invención;
las figuras 2A y 2B son diagramas de bloques del dispositivo médico y el controlador de acuerdo con una realización ilustrativa de la presente invención;
la figura 3 representa componentes de radiofrecuencia (RF) del dispositivo médico y el controlador representados en las figuras 2A y 2B y de acuerdo con una realización ilustrativa de la presente invención; y
las figuras 4, 5 y 6 son diagramas de señales transmitidas desde el dispositivo médico y el controlador de acuerdo con una realización de la presente invención;
las figuras 7A y 7B son diagramas de operaciones del dispositivo médico y el controlador representados en las figuras 2A y 2B y de acuerdo con una realización ilustrativa de la presente invención; y
las figuras 8A y 8B son diagramas de operaciones del dispositivo médico y el controlador representados en las figuras 2A y 2B y de acuerdo con otra realización ilustrativa de la presente invención.
la figura 9 es un diagrama de operaciones de dispositivos homólogos que emplean generación de claves fuera de banda (OOB) integrada, para un emparejamiento inalámbrico seguro de acuerdo con una realización ilustrativa de la presente invención.

A lo largo de las figuras de dibujos, se comprenderá que los números de referencia similares se refieren a elementos, características y estructuras similares.

DESCRIPCIÓN DETALLADA DE REALIZACIONES ILUSTRATIVAS

A continuación se hará referencia en detalle a las realizaciones de la presente invención, que se ilustran en los dibujos adjuntos. Las realizaciones descritas en la presente memoria ejemplifican, pero no limitan, aspectos de la presente invención haciendo referencia a los dibujos.

Haciendo referencia a las figuras 1, 2A y 2B, se muestra un sistema de administración de medicamentos 10 ilustrativo que tiene un dispositivo médico 12 y un controlador 14 con pantalla 24 u otra interfaz de usuario.

El dispositivo médico 12 puede ser un dispositivo ponible o un dispositivo transportado por un paciente. El dispositivo médico 12 puede tener una interfaz de usuario integrada como su controlador 14, o el dispositivo médico puede

estar configurado para ser controlado por un dispositivo controlador independiente, tal como un controlador inalámbrico 14, como se muestra en la figura 1. En la realización ilustrada, el dispositivo médico 12 está controlado por un controlador inalámbrico 14, pero debe entenderse que los aspectos de las realizaciones ilustrativas de la presente invención aplican a un dispositivo médico 12 con su propio controlador y otro dispositivo 14 a emparejar con el dispositivo médico 12. Además, el controlador inalámbrico 14 puede ser un teléfono inteligente, por ejemplo.

Por ejemplo, el dispositivo médico 12 puede ser un dispositivo de administración de insulina (IDD) desechable para uso en un solo paciente, que está configurado para la administración subcutánea continua de insulina a velocidades basales fijas y variables (período de 24 horas) y dosis en bolo (bajo demanda) para el tratamiento de pacientes con diabetes mellitus de tipo 2 (T2DM) que requieren terapia con insulina. Debe entenderse, sin embargo, que el dispositivo médico 12 puede ser cualquier dispositivo médico corporal (por ejemplo, bomba de infusión ponible, medidor continuo de glucosa) o dispositivos médicos de red de área corporal (BAN) (por ejemplo, medidor portátil de glucosa en sangre, teléfono inteligente con aplicaciones de tratamiento de afecciones médicas, o controlador inalámbrico para dispositivo corporal).

Como se describe a continuación, se describe un proceso de generación de claves OOB integrada, de acuerdo con una realización ilustrativa de la presente invención y haciendo referencia a la figura 9, que mejora la seguridad de un protocolo de emparejamiento estándar BLE ilustrado en la figura 7B o la figura 8B. Debe entenderse que el proceso de emparejamiento previo basado en rango, descrito en relación con la figura 7A o la figura 8A, no tiene por qué implementarse a través de los dispositivos 12 y 14 para un emparejamiento con el fin de obtener los beneficios del proceso de generación de claves OOB de la figura 9. Se emplea la opción de emparejamiento OOB del protocolo de emparejamiento estándar BLE, ya que proporciona más seguridad que las opciones de emparejamiento Funciona directamente y Entrada con clave de paso de BLE.

También haciendo referencia continua a las figuras 1, 2A y 2B, el IDD 12 es parte de un sistema 10 que es un sistema avanzado de suministro de insulina para uso de pacientes con diabetes mellitus de tipo 2 (T2DM). Este está configurado para su uso las 24 horas del día en todos los entornos habitados normalmente por los usuarios previstos. Está configurado para que el usuario paciente lleve puesto el IDD durante un período de tres días (hasta 84 horas). Tiene cuatro (4) funciones principales: suministrar una tasa de insulina basal diaria establecida por el usuario; administrar la cantidad de insulina en bolo establecida por el usuario; administrar una o varias dosis de insulina en bolo manual; y generar notificaciones y estado del sistema. El sistema aborda una necesidad insatisfecha, de muchos pacientes de tipo 2 , de inyecciones diarias (MDI), que demanda una administración de insulina discreta, simple y eficaz, alternativa a la bomba de insulina compleja tradicional. Sin embargo, debe entenderse que el dispositivo médico 12 se puede usar para administrar cualquier tipo de fluido y no se limita a la administración de insulina.

El Controlador Inalámbrico (WC) 14 se utiliza para programar el IDD que se lleva puesto en el cuerpo, para administrar al paciente una tasa de insulina basal diaria y una cantidad de insulina a la hora de las comidas. El WC 14 también proporciona información de estado del IDD 12 así como notificaciones al usuario. El IDD 12 que se lleva puesto en el cuerpo almacena y administra insulina al paciente por vía subcutánea. El IDD envía retroalimentación al paciente a través del WC si detecta problemas (por ejemplo, volumen bajo en el depósito, batería baja). Una función importante soportada por el software de comunicación en el sistema 10 es la comunicación inalámbrica entre el WC 14 y el IDD 12, que permite que el IDD 12 proporcione retroalimentación al WC 14 y que el usuario controle su administración de insulina mediante el IDD 12 de forma inalámbrica por medio del WC 14 de forma sencilla y discreta.

En la realización ilustrada mostrada en la figura 2A, el IDD 12 tiene un microcontrolador 60 configurado para controlar un mecanismo de bombeo 52, la comunicación inalámbrica con el WC (por ejemplo, a través de un circuito de RF 54 que tiene un circuito de adaptación y una antena) y las operaciones de bombeo. El IDD tiene uno o más botones 64 de bolo para la administración manual de medicación además de la administración programada de medicación. El mecanismo de bombeo 52 comprende un depósito 76 para almacenar un medicamento fluido (por ejemplo, insulina) para administrarlo a través de una cánula 68 al paciente que lleva puesto el IDD, y una bomba 72 para administrar de forma controlable cantidades designadas de medicamento, desde el depósito a través de la cánula. El depósito 76 se puede llenar a través de un tabique 78 utilizando una jeringa. El IDD tiene un mecanismo de inserción manual 66 para insertar la cánula 68 en un paciente; sin embargo, el procesador 60 puede configurarse para hacer funcionar un circuito de activación opcional para automatizar la operación del mecanismo de inserción 66 para desplegar la cánula 68 en el paciente. Además, el IDD 12 puede estar dotado opcionalmente de un sensor de fluido 74 o un sensor de presión 70. El microcontrolador 60 puede hacer funcionar un LED 62 para que esté encendido o parpadee durante una o más operaciones de bombeo, tal como durante el cebado del depósito, por ejemplo. El IDD 12 es alimentado por una batería y un regulador, como se indica en 58. Al inicializar el IDD 12 (por ejemplo, al encenderlo para comenzar el emparejamiento con el WC 12), el o los botones de bolo 64 se pueden configurar como uno o varios botones de activación que, cuando son activados por el usuario, hacen que el IDD 12 se active desde un modo de estante de conservación de energía.

En la realización ilustrada mostrada en la figura 2B, el WC 14 se implementa como un componente de microprocesador dual que tiene: 1) un procesador principal de WC (WCMP) 30 y un procesador de comunicaciones

de WC (WCCP) 32. El WCMP 30 está conectado a los componentes de interfaz de usuario (UI) tales como la pantalla LCD con pantalla táctil 24, uno o más botones 28, un indicador LED 26 y similares. El WCCP 32 está conectado a componentes de radiofrecuencia (RF) 38 (por ejemplo, una antena y un circuito de adaptación) y es principalmente responsable de la comunicación inalámbrica del WC 14 con el IDD 12. Los dos procesadores 30, 32 se comunican entre sí a través de una Interfaz periférica en serie (SPI). Los dos procesadores 30, 32 también pueden interrumpirse entre sí a través de dos patillas de interrupción, M_REQ_INT y S_REQ_INT.

También haciendo referencia a la figura 2B, el WC 14 está diseñado para que su mantenimiento no se tenga que realizar in situ (es decir, el usuario no tiene que inspeccionar, ajustar, reemplazar o mantener partes), excepto las baterías alcalinas reemplazables 34 para la alimentación. Una memoria no volátil (por ejemplo, una memoria flash) está dispuesta 36 en el WC para almacenar datos de estado y entrega recibidos del IDD 12, tales como fechas y horas de entrega, y cantidades.

La LCD con pantalla táctil capacitiva 24 sirve como interfaz visual para el usuario al presentar salidas visuales y gráficas al usuario (por ejemplo, información del sistema, instrucciones, avisos visuales, configuraciones de usuario, salidas de datos, etc.), y al disponer una interfaz de visualización para que el usuario introduzca entradas (por ejemplo, entradas de operación del dispositivo, tales como emparejamiento y configuración y dosificación de IDD, y parámetros de configuración, etc.). La pantalla de WC con pantalla táctil capacitiva 24 detecta (al menos) gestos de un solo toque sobre su área de visualización. Por ejemplo, la pantalla táctil está configurada para reconocer entradas táctiles del usuario (tocar, deslizar y presionar un botón), lo que permite la navegación dentro de las pantallas y aplicaciones de la UI. La pantalla táctil 24 ayuda a ejecutar funcionalidades específicas del sistema (es decir, configuración y emparejamiento de IDD 12 con el WC 14, dosificación de insulina, proporcionar al usuario un historial de dosificación y desactivación y reemplazo de IDD por otro IDD, etc.) a través de interacciones específicas con el usuario. El WC 14 también puede incluir un botón 28 tal como un botón de activación del dispositivo que, cuando es activado por el usuario, hace que el WC 14 se active de un modo de reposo de ahorro de energía. El WC 14 también puede tener un LED 26 para indicar un estado de batería baja (por ejemplo, indicar el estado de batería baja cuando quedan 12 o menos horas de uso).

La interfaz de radiofrecuencia (RF) del WC 14 con el IDD 12 se basa, por ejemplo, en un protocolo de comunicación Bluetooth® de baja energía o en BLE, aunque se pueden utilizar otros protocolos de comunicación inalámbrica. En el sistema de administración de medicamentos 10, el WC 14 y el IDD 12 se comunican de forma inalámbrica dentro de una distancia de hasta 10 pies o aproximadamente 3 metros, utilizando la banda ISM del espectro de 2400 MHz a 2480 MHz. El WC 14 comunica con el IDD 12 mientras el IDD está adherido al cuerpo al aire libre. El WC 14 es el dispositivo central o maestro, y el IDD 12 es el dispositivo periférico o esclavo. Cada vez que el WCMP 30 quiere enviar información al IDD 12 o recuperar información del IDD 12, lo hace interactuando con el WCCP 32, que, a su vez, se comunica con el IDD 12 a través del enlace BLE a través de los respectivos circuitos de RF 38 y 54, como se muestra en la figura 3.

De acuerdo con una realización ilustrativa de la presente invención, el WC 14 (por ejemplo, su WCCP 32) y el IDD 12 se comunican de acuerdo con un protocolo y varias operaciones para mitigar el riesgo de que el WC 14 se empareje con un IDD 12' no deseado o, viceversa, que un IDD 12 previsto se empareje con un WC 14' no previsto. Cualquiera de los casos podría provocar un funcionamiento no intencionado del mecanismo de bomba 53, teniendo potencialmente como resultado una sobreinfusión de insulina que puede ser perjudicial para el paciente. De acuerdo con aspectos ilustrativos del sistema 10, el rango de comunicación en el inicio de IDD 12 (por ejemplo, antes del emparejamiento) se reduce, los dispositivos no deseados tales como un IDD 12' no deseado son rechazados por el WC 14 y, cuando se detectan en el entorno coexistencias de múltiples IDD, se impide que el WC 14 se empareje con un IDD 12 a menos que ese IDD 12 sea el único IDD detectado por el WC 14. Como se describe con más detalle a continuación, las operaciones de ejemplo en el sistema 10 comprenden reducir el nivel de potencia de transmisión del WC 14 y el IDD 12 para controlar el rango de comunicación (por ejemplo, a menos o igual a 20" antes del emparejamiento), utilizar indicadores de intensidad de la señal (por ejemplo, umbrales mínimo y máximo de indicador de intensidad de la señal recibida (RSSI)) para rechazar los dispositivos no deseados, incluidos los IDD no deseados 12', ajustar el tiempo de escaneo de inicio del WC 14 para detectar la coexistencia de múltiples IDD, instruir al usuario para que se traslade a otra habitación o ubicación con su WC 14 e IDD 12 para volver a intentar el emparejamiento cuando haya más de un IDD 12 detectado, y solo permite que el WC 14 se empareje con el IDD 12 cuando es el único IDD 12 detectado por el WC 14.

El anuncio de IDD 12 y el escaneo de WC 14 antes del emparejamiento se ilustran en la figura 4 y de acuerdo con una realización ilustrativa de la presente invención. Tras la activación y antes del emparejamiento, cada 250 ms (+/- 10 %) tal como se indica en 106, el IDD 12 se anuncia con paquetes de datos de anuncio de inicio de IDD 100 y espera 3 ms (+/- 10 %) para la posible respuesta desde un WC 14. Con la solicitud del WCMP 30, el WCCP 32 inicia la comunicación comenzando a escanear el anuncio de IDD cada 746 ms (+/- 10 %) 104 durante aproximadamente una ventana de escaneo 102 de 505 ms (+/- 10 %). Al final del período de escaneo 104, el WCCP 32 realiza una verificación de coexistencia, tal como se describe a continuación en relación con las figuras 7 y 8. Al final del período de tiempo de escaneo 104, si el WCCP 32 no detecta ningún paquete de anuncio 100 dentro de un período de límite de tiempo de la capa de transporte, el WCCP deja de escanear y envía una respuesta Nack con un código de error

de límite de tiempo de transmisión. Como se describe a continuación en relación con las figuras 7 y 8, después de enviar una respuesta Nack, el WCCP 32 entra en reposo si no se detecta anuncio.

El anuncio de IDD 12 y el escaneo de WC 12 después del emparejamiento se ilustran en la figura 5 y de acuerdo con una realización ilustrativa de la presente invención. Después del emparejamiento, si el IDD 12 no está bombeando activamente, se anuncia con un paquete de datos periódicos IDD 100 en un intervalo seleccionado 108 (por ejemplo, cada 1 segundo (+/- 10%). Después de cada anuncio 100, el IDD 12 espera 30 ms (+/- 10 %) para la posible respuesta del WC 14. Después del emparejamiento, con la solicitud del WCMP 30, el WCCP 32 inicia la comunicación comenzando a escanear el anuncio de IDD cada 746 ms (+/- 10 %) 104 durante una ventana de escaneo de 505 ms (+/- 10 %) 102.

El anuncio de IDD 12 y el escaneo de WC 14 durante el bombeo se ilustran en la figura 6 y de acuerdo con una realización ilustrativa de la presente invención. Si el IDD 12 está administrando un medicamento como insulina, se anuncia cada 500 ms durante 2 segundos al final de un recorrido de dispensación 112. Aunque no se indica en la figura 6, durante el tiempo de descanso entre los períodos de aspiración del IDD 110 y los períodos de dispensación 112 del IDD, el IDD 12 sigue intentando anunciarse si es posible. Cuando el IDD 12 está bombeando, con la solicitud del WCMP 30, el WCCP 32 inicia la comunicación comenzando a escanear el anuncio de IDD cada 746 ms (+/- 10 %) 104 durante ventanas de escaneo 102 de 505 ms (+/- 10 %).

Haciendo referencia a las figuras 7A y 7B, se describen las operaciones para el WC 14 y el IDD 12 y en particular con respecto al WCMP 30, el WCCP 32 y el procesador 60 del IDD. Se muestra una interfaz SPI entre el WCMP 30 y el WCCP 32; sin embargo, como se explicó anteriormente, el WC 14 se puede configurar como un dispositivo de un solo procesador. Además, como se describió anteriormente, está dispuesta una interfaz BLE o una interfaz inalámbrica similar 124 entre el WC 14 y el IDD 60. Las operaciones están numeradas del 1 al 30 en las figuras 7A y 7B para facilitar la referencia.

Para comenzar a emparejar el WC 14 con un IDD 12, el IDD 12 puede activarse desde un modo de estante de conservación de energía (por ejemplo, mediante la activación de uno o varios botones 64 por del usuario), como se indica en la operación 1 en la figura 7A. El IDD 12 reduce su potencia de transmisión (operación 2) y comienza a anunciar datos de anuncio de inicio de IDD (operación 5) con el nivel de potencia de transmisión 0 hasta 1 minuto +/- 10%. El IDD 12 transmite periódicamente un paquete de datos de anuncio de inicio de IDD (operación 8). El WC 14 puede activarse desde su modo de reposo de ahorro de energía (por ejemplo, como se indica en la operación 3) en respuesta a que un usuario active un botón, tal como un botón de inicio de la pantalla táctil 24 u otro botón 28, y entre en un modo de inicio (operación 4), tal como el WCMP 30 enviando un comando de inicio al WCCP 32. Al recibir el comando de inicio, el WCCP 32 comienza a escanear los datos de anuncio de inicio de IDD (operación 6) como ha descrito anteriormente en relación con la figura 4.

También haciendo referencia a la figura 7A ya la operación 9, el WC 14 puede determinar si un tipo particular de dispositivo 12 está cerca. Por ejemplo, los datos de anuncio de inicio de IDD 12 pueden comprender información de identificación de IDD (por ejemplo, parámetros o valores dinámicos y/o estáticos seleccionados que identifican un tipo de dispositivo, tal como fabricante y/o modelo u otra característica) de modo que el WC 14 puede ser configurado para emparejarse solo con dispositivos o IDD que tengan información de identificación de IDD designada y no con otros dispositivos que tengan la información de identificación de IDD designada. Haciendo referencia a la operación 9, el WCCP 32 puede determinar si los datos de anuncio de inicio de IDD 12 tienen información de identificación de IDD relacionada, por ejemplo, con su fabricante particular. Si no, el WCCP 32 continúa escaneando (operación 7).

Haciendo referencia a la operación 10 en la figura 7A, si el WCCP 32 escanea los datos de anuncio de inicio de IDD desde un dispositivo cercano que tiene la información de identificación de IDD designada, entonces el WCCP 32 comienza a determinar si la información de intensidad de la señal relativa a los datos de anuncio de inicio de IDD satisface uno o más umbrales. Por ejemplo, el WCCP 32 puede dejar de escanear y realizar una verificación del indicador de intensidad de la señal de recepción (RSSI) en el paquete recibido. La información de RSSI se puede generar, por ejemplo, mediante un chip de RF en el circuito de RF 38 del WC 14. Si el RSSI es inferior a un nivel mínimo (por ejemplo, - 65 dBm +/- 10 %), el WCCP 32 ignora el paquete de anuncio recibido y vuelve a intentar el proceso de escaneo (operación 7). El nivel mínimo se selecciona para diferenciar un anuncio IDD 12 en las cercanías del WP 14, respecto de ruido o de un IDD 12 que está lo suficientemente lejos del WC 14 como para ser un dispositivo no deseado para emparejamiento.

Haciendo referencia a la operación 11 en la figura 7A, si el RSSI está por encima de un nivel máximo (por ejemplo, -3 dBm +/- 10 %), tal como cuando puede haber ocurrido un bloqueo de RF, el WCCP 32 envía una respuesta Nack al WCMP 30 (por ejemplo, una respuesta con un código de error de RSSI máximo excedido), tal como se indica en la operación 12. El WCMP 30 puede, a su vez, generar una alerta (por ejemplo, a través de la pantalla táctil LCD 24) para advertir al usuario de que se desplace a otra ubicación (operación 13).

Si, al final del período de tiempo de escaneo, el WCCP 32 detecta los paquetes de anuncio de más de un IDD 12 (operación 14), el WCCP 32 envía una respuesta Nack al WCMP 30 (por ejemplo, una respuesta con un código de

error de coexistencia detectada(operación 15). El WCMP 30 puede, a su vez, generar una alerta (por ejemplo, a través de la pantalla táctil LCD 24) para advertir al usuario de que se desplace a otra ubicación para volver a intentar el emparejamiento y, opcionalmente, de que se ha detectado otro IDD (operación 16).

Si las comprobaciones de RSSI y coexistencia han pasado, el WCCP 32 puede enviar un mensaje de respuesta de datos de anuncio de inicio de IDD al WCMP 30 (operación 17). Al recibir el mensaje de respuesta, el WCMP 30 verifica los datos de anuncio de inicio de IDD (por ejemplo, utilizando la información de identificación de IDD designada) (operación 18). Si esta comprobación de compatibilidad de IDD es satisfactoria, el WCMP 30 envía un mensaje de comando de emparejamiento al WCCP 32 (operación 19). Al recibir el comando de emparejamiento, el WCCP 32 puede realizar una verificación de normalidad de IPC en el mensaje de comando de emparejamiento antes de realizar la generación de claves fuera de banda (OOB) (operación 20) de acuerdo con realizaciones ilustrativas de la presente invención.

Haciendo referencia a la operación 21 en la figura 7A, se inicia un proceso de emparejamiento (por ejemplo, el método de emparejamiento OOB de Bluetooth de baja energía) entre el IDD 12 y el WC 14. Por ejemplo, como se indica en las operaciones 22 y 23 en la figura 7B, el IDD 12 puede recibir una solicitud de emparejamiento y realizar una verificación de normalidad que hace que el IDD 12 ignore la solicitud si falla la verificación de normalidad y envíe una respuesta de emparejamiento al WCCP 32 si la verificación de normalidad tiene éxito. El IDD 12 y el WCCP 32 pueden realizar cada uno un algoritmo de emparejamiento (operación 24) (por ejemplo, emparejamiento Bluetooth de baja energía (BLE)). Las claves de emparejamiento se pueden generar en el IDD 12 y el WCCP 32 por separado, de modo que no se necesita la interfaz aérea para el intercambio de claves de emparejamiento. El WCCP 32 guarda la información de la clave de emparejamiento en una ubicación de memoria no volátil. El WCCP 32 confirma el emparejamiento enviando un paquete de confirmación de nivel bajo al IDD (operación 25). Al recibir el paquete de confirmación del WCCP 32, el IDD 12 guarda la información de la clave de emparejamiento. Al recibir el paquete de confirmación del WCCP, el IDD confirma el emparejamiento enviando un paquete de confirmación de nivel bajo, de retorno al WCCP 32 (operación 26). Así, el WCCP 14 y el IDD 32 facilitan la distribución de claves de emparejamiento (operación 27).

También haciendo referencia a la figura 7B, una vez completado el emparejamiento (por ejemplo, de acuerdo con el emparejamiento del protocolo de administrador de seguridad (SMP) estándar BLE), el WCCP 32 envía un comando de emparejamiento al IDD 12 (por ejemplo, para realizar emparejamiento de la capa de transporte una vez se completa el emparejamiento de nivel bajo) (operación 28). Al recibir el paquete de confirmación del IDD, el WCCP 32 envía el mensaje de emparejamiento satisfactorio al WCMP 30 (operación 29). Al recibir el mensaje de emparejamiento satisfactorio, el WCMP 30 guarda la información de la clave de emparejamiento en una ubicación de memoria no volátil para el registro y puede mostrar el emparejamiento satisfactorio en una interfaz de usuario (operación 30). Después del emparejamiento, el nivel de potencia de transmisión del IDD se ajusta (por ejemplo, en 15) para aumentar el rango de comunicación (operación 31). Además, después del emparejamiento, también se incrementa el nivel de potencia de transmisión del WCCP 32. El WC 14 solo comunica con el IDD 12 emparejado, y el IDD 12 solo acepta un comando del WC 14 emparejado. Esta relación de comunicación vinculada del WC 12 y el IDD 14 permanece hasta que se desactiva el IDD. Después de la desactivación del IDD, el WC 14 puede emparejarse con un nuevo IDD 12; sin embargo, en un momento dado, preferiblemente solo se permite al WC 14 emparejarse con un IDD 12.

Las operaciones del WC 14 y el IDD 12 en las figuras 8A y 8B son similares a las de las figuras 7A y 7B, excepto que la comprobación de coexistencia (operación 10) se produce antes de las comprobaciones de intensidad de la señal (por ejemplo, RSSI) (operaciones 13 y 14). En otras palabras, el orden de las comprobaciones de coexistencia y de intensidad de la señal puede ser intercambiable. Además, la verificación del dispositivo (operación 9) puede ser opcional.

De acuerdo con un aspecto de la presente invención, el WCCP 32 no necesita escanear constantemente (por ejemplo, la operación 7 de las figuras 7A y 8A), lo que ahorra energía del WC 14. En otras palabras, el escaneo por el WCCP se puede intercalar de manera que el escaneo se produzca durante una duración seleccionada (por ejemplo, una ventana de escaneo 102 de 505 ms como se muestra en la figura 4) que es más larga que dos intervalos de anuncio 106 (por ejemplo, dos intervalos de anuncio 106 de 250 ms) por el IDD 12 para garantizar que el WCCP 32 no pierda la detección de un paquete de datos de anuncio de inicio de IDD 100 de un IDD 12 dentro del rango de emparejamiento del WC 14. El WCCP detiene a continuación el escaneo durante un intervalo de tiempo seleccionado (por ejemplo, 241 ms en la figura 4) dentro de un intervalo de escaneo 104 antes de escanear de nuevo durante otra ventana de escaneo 102 de tiempo dentro del siguiente intervalo de escaneo 104.

Si se detecta un paquete de datos de anuncio de inicio de IDD 100 durante una ventana de escaneo 102, entonces el WCCP 32 deja de escanear y comienza una o más de las diversas comprobaciones descritas anteriormente en relación con la figura 7A; es decir, una verificación del dispositivo (operación 9), verificaciones de intensidad de la señal recibida (operaciones 10 y 11) y una verificación de coexistencia (operación 14). Si se localizan múltiples dispositivos a través de la operación 14, o no se pasan las otras comprobaciones (es decir, las operaciones 9, 10 y 11), entonces el WCCP 32 comienza a escanear de nuevo (operación 7).

Si no se detecta un paquete de datos de anuncio de inicio de IDD 100 durante una ventana de escaneo 102, entonces el WCCP 32 puede escanear en una serie de intervalos de escaneo 104 durante una cantidad de tiempo seleccionada (por ejemplo, 10 segundos) y a continuación alcanzar el límite de tiempo. Tras alcanzar el límite de tiempo, el WCCP 32 puede enviar una señal Nack al WCMP 30 que, a su vez, alerta al usuario sobre un error de comunicación y la necesidad de cerrar un IDD 12 previsto al WC 14 y de volver a intentar el emparejamiento.

De acuerdo con un aspecto de la presente invención y haciendo referencia a la figura 9, se describirá a continuación una mejora (por ejemplo, la operación 20 en la figura 7A y la figura 8A) del emparejamiento estándar BLE ilustrado en las figuras 7B y 8B, para aumentar la seguridad utilizando generación de claves OOB. En primer lugar, se utiliza un algoritmo resumen seguro (H) como, por ejemplo, AES-128 o SHA-256 u otro algoritmo resumen seguro, en cada uno de los dispositivos homólogos que se van a emparejar. En segundo lugar, las entradas de la función resumen para los dispositivos homólogos se configuran para que sean las mismas, de modo que se pueda generar una clave OOB idéntica como salida de la función resumen en cada uno de los dispositivos homólogos. Con el fin de construir las mismas entradas para la función resumen en cada dispositivo homólogo, un dispositivo homólogo (por ejemplo, IDD 12) transmite algunos de sus datos únicos a otro dispositivo homólogo (por ejemplo, el controlador inalámbrico 14) para compartir (es decir, en lo sucesivo denominados datos compartidos) como, por ejemplo, una dirección MAC y/u otros parámetros únicos dinámicos, mediante anuncios 100. Además, todos los dispositivos que pueden ser emparejados potencialmente (por ejemplo, los IDD 12, WC o aplicaciones de teléfono inteligente 14) comparten una credencial, por ejemplo, una clave secreta de 128 bits. Usando estos datos compartidos y la clave secreta predefinida en la función resumen segura como entrada, ambos dispositivos homólogos 12, 14 generan una clave OOB idéntica de 128 bits, es decir, los datos de autenticación para el emparejamiento. Los parámetros dinámicos como la dirección MAC se pueden construir como una variante (por ejemplo, única entre los IDD 12), y la clave secreta de 128 bits se comparte y se mantiene igual (por ejemplo, la misma que entre los IDD 12 y WC o aplicaciones de teléfono inteligente 14). Por lo tanto, la clave OOB para cada par 12, 14 de varios conjuntos de dispositivos de emparejamiento es diferente y segura.

Como se muestra en la figura 9, un dispositivo esclavo (por ejemplo, el IDD 12) y un dispositivo maestro (por ejemplo, el controlador inalámbrico 14) son ambos dotados de una clave secreta predefinida (C) y una función resumen segura (H). Por ejemplo, ambos dispositivos maestro y esclavo están programados con una clave secreta idéntica de 16 bytes C = {c0, c2, ... c15}. La clave secreta C y la función resumen H se pueden proporcionar, por ejemplo, a los IDD y WC 14 en el momento de la fabricación, o a un teléfono inteligente 14 que funciona con el IDD en el momento en que se instala la aplicación correspondiente que contiene esta información necesaria para la generación de claves. El dispositivo esclavo prepara sus datos compartidos únicos {*s1, s2, s3,* ..., *sn}.* Como se indica en 120, cada IDD 12 está configurado para transmitir paquetes de anuncio 100 a un WC 14 con el que desea emparejarse. Los paquetes de anuncio 100 contienen datos compartidos únicos de ese IDD... s1, s2,... , sn. Como se indica en 119, el dispositivo maestro comienza a escanear y el dispositivo esclavo anuncia los datos compartidos {*s1, s2, s3,* ..., *sn}.* El dispositivo maestro lee los datos compartidos de los anuncios del esclavo, como se indica en 121, de modo que tanto el IDD como el WC calculan la misma entrada S = s1 || s2 || s3 || .... || sn, como se indica en 122. Las mismas entradas (es decir, datos compartidos S y clave predefinida C) se proporcionan al mismo algoritmo resumen seguro seleccionado H, proporcionado en cada uno de los dispositivos homólogos, como se indica en 124, de modo que el IDD 12 y cada WC 14 generan claves idénticas, como se indica en 126 (es decir, Km = H(C, S) y Ks = H(C, S); por lo tanto, Km = Ks). Por lo tanto, los datos OOB que comprenden una clave se proporcionan en cada uno de los dispositivos homólogos para comenzar el emparejamiento OOB con Km y Ks respectivamente, como se indica en 128.

La generación de claves OOB descrita en relación con la figura 9 y de acuerdo con una realización ilustrativa de la presente invención presenta una serie de ventajas. En primer lugar, se impiden los ataques de intermediario y las escuchas ilegales mediante el uso de un método de generación de claves OOB. En segundo lugar, no se necesita capacidad de IO, lo que permite IDD 12 simplificados y menos costosos u otros dispositivos médicos que no requieran, por ejemplo, un teclado numérico y/o pantalla para introducir datos de autenticación. Por lo tanto, la opción de emparejamiento más segura de BLE (es decir, emparejamiento OOB) se consigue sin una capacidad de E/S en ninguno de los dispositivos homólogos. La generación de claves OOB descrita en este documento de acuerdo con realizaciones ilustrativas de la presente invención también impide los cálculos de fuerza bruta dado que el algoritmo de generación de claves OOB se basa tanto en entradas dinámicas como estáticas y, por lo tanto, aumenta la dificultad de los cálculos de fuerza bruta.

Un experto en la técnica entenderá que esta descripción no se limita en su aplicación a los detalles de construcción y la disposición de los componentes expuestos en la siguiente descripción o ilustrados en los dibujos. Las realizaciones del presente documento son susceptibles de otras realizaciones, y susceptibles de practicarse o llevarse a cabo de varias formas. Además, se entenderá que la fraseología y la terminología utilizadas en el presente documento tienen fines descriptivos y no deben considerarse limitativas. El uso de "que incluye", "que comprende" o "que tiene" y variaciones de los mismos en este documento pretende abarcar los elementos enumerados a continuación y sus equivalentes, así como elementos adicionales. A menos que se limiten de otro modo, los términos "conectado", "acoplado" y "montado" y variaciones de los mismos en el presente documento se usan ampliamente y abarcan conexiones, acoplamientos y montajes directos e indirectos. Además, los términos "conectado" y "acoplado" y variaciones de los mismos no se limitan a conexiones o acoplamientos físicos o

mecánicos. Además, términos tales como arriba, abajo, parte inferior y parte superior son relativos y se emplean para ayudar a ilustrar, pero no son limitativos.

Los componentes de los dispositivos, sistemas y métodos ilustrativos empleados de acuerdo con las realizaciones ilustradas de la presente invención pueden implementarse, al menos en parte, en circuitos electrónicos digitales, circuitos electrónicos analógicos o en hardware informático, software inalterable, software o en combinaciones de los mismos. Estos componentes pueden implementarse, por ejemplo, como un producto de programa informático, tal como un programa informático, código de programa o instrucciones informáticas, incorporados tangiblemente en un soporte de información, o en un dispositivo de almacenamiento legible por máquina, para ser ejecutado por, o controlar el funcionamiento de, aparatos de procesamiento de datos tales como un procesador programable, un ordenador o varios ordenadores.

Un programa informático se puede escribir en cualquier forma de lenguaje de programación, incluyendo lenguajes compilados o interpretados, y se puede implementar de cualquier forma, incluyendo un programa independiente o como un módulo, componente, subrutina u otra unidad adecuada para su uso en un entorno informático. Un programa informático puede implementarse para ejecutarse en un ordenador o en varios ordenadores en un sitio o distribuirse en varios sitios e interconectarse mediante una red de comunicación. Además, los programas, códigos y segmentos de código funcionales para realizar realizaciones ilustrativas de la presente invención pueden interpretarse fácilmente como dentro del alcance de la invención por programadores expertos en la técnica a la que pertenece la presente invención. Las etapas del método asociadas con las realizaciones ilustrativas de la presente invención pueden ser realizadas por uno o más procesadores programables que ejecutan un programa, código o instrucciones informáticas para realizar funciones (por ejemplo, operando con datos de entrada y/o generando una salida). Las etapas del método también pueden ser realizadas por, y el aparato de las realizaciones ilustrativas de la presente invención se puede implementar como un circuito lógico de propósito especial, por ejemplo, una FPGA (field programmable gate array, matriz de puertas programables en campo) o un ASIC (application-specific integrated circuit, circuito integrado de aplicación específica), por ejemplo .

Los diversos bloques, módulos y circuitos lógicos ilustrativos descritos en relación con las realizaciones dadas a conocer en este documento pueden implementarse o realizarse con un procesador de propósito general, un procesador de señal digital (DSP), un ASIC, una FPGA u otro dispositivo lógico programable, puerta discreta o lógica de transistores, componentes de hardware discretos o cualquier combinación de los mismos diseñada para realizar las funciones descritas en este documento. Un procesador de propósito general puede ser un microprocesador, pero como alternativa, el procesador puede ser cualquier procesador, controlador, microcontrolador o máquina de estado convencional. Un procesador también puede implementarse como una combinación de dispositivos informáticos, por ejemplo, una combinación de un DSP y un microprocesador, una pluralidad de microprocesadores, uno o más microprocesadores junto con un núcleo DSP o cualquier otra configuración similar.

Los procesadores adecuados para la ejecución de un programa de ordenador incluyen, a modo de ejemplo, tanto microprocesadores de propósito general como de propósito especial, y uno o más procesadores de cualquier tipo de ordenador digital. Generalmente, un procesador recibirá instrucciones y datos de una memoria de solo lectura o de una memoria de acceso aleatorio o de ambas. Los elementos esenciales de un ordenador son un procesador para ejecutar instrucciones y uno o más dispositivos de memoria para almacenar instrucciones y datos. Generalmente, un ordenador también incluirá, o estará acoplado operativamente para recibir datos de, o transferir datos a, o ambos, uno o más dispositivos de almacenamiento masivo para almacenar datos, por ejemplo, discos magnéticos, magneto-ópticos o discos ópticos. Los soportes de información adecuados para incorporar instrucciones y datos de programas informáticos incluyen todas las formas de memoria no volátil, incluyendo, a modo de ejemplo, dispositivos de memoria semiconductores, por ejemplo, memoria de solo lectura programable eléctricamente o ROM (EPROM), ROM programable borrable eléctricamente (EEPROM) , dispositivos de memoria flash y discos de almacenamiento de datos (por ejemplo, discos magnéticos, discos duros internos o discos extraíbles, discos magnetoópticos y discos CD-ROM y DVD-ROM). El procesador y la memoria pueden complementarse con, o incorporarse a un circuito lógico de propósito especial.

Los expertos en la técnica comprenderán que la información y las señales pueden representarse usando cualquiera de una variedad de tecnologías y técnicas diferentes. Por ejemplo, los datos, instrucciones, comandos, información, señales, bits, símbolos y chips a los que se puede hacer referencia a lo largo de la descripción anterior pueden estar representados por voltajes, corrientes, ondas electromagnéticas, campos magnéticos o partículas, campos ópticos o partículas, o cualquier combinación de los mismos.

La descripción y las figuras presentadas anteriormente están concebidas solo como ejemplo y no para limitar la presente invención en modo alguno, excepto tal como se establece en las siguientes reivindicaciones. Se observa particularmente que los expertos en la materia pueden combinar fácilmente los diversos aspectos técnicos de los diversos elementos de las diversas realizaciones ilustrativas que se han descrito anteriormente de muchas otras formas, todas las cuales se consideran dentro del alcance de la invención.

**REIVINDICACIONES**

1. Un método de generación de claves para emparejar de forma segura un primer dispositivo (12) con un segundo dispositivo (14) para una comunicación inalámbrica entre ambos, que comprende:

proporcionar inicialmente a cada uno del primer dispositivo (12) y el segundo dispositivo (14) una credencial y una función resumen;
después de dicha etapa de provisión inicial, el primer dispositivo (12) transmite señales de anuncio a intervalos seleccionados y en un rango de radiofrecuencia seleccionado, a través de una primera antena;
el segundo dispositivo (14) escanea la radiofrecuencia seleccionada a través de una segunda antena;
el primer dispositivo (12) proporciona datos a compartir con el segundo dispositivo (14) en las señales de anuncio;
el segundo dispositivo (14) recibe los datos compartidos a través del escaneo;
**caracterizado por que**
el segundo dispositivo (14) y el primer dispositivo (12) utilizan, cada uno, los datos compartidos y la credencial como entrada a la función resumen para generar una clave fuera de banda, OOB, siendo idéntica la clave OOB generada por el primer dispositivo (12) a la clave OOB generada por el segundo dispositivo (14); y
el segundo dispositivo (14) y el primer dispositivo (14) realizan el emparejamiento OOB entre sí usando su respectiva clave OOB antes de realizar emparejamiento estándar Bluetooth de baja energía, BLE, en el que el segundo dispositivo y el primer dispositivo realizan, cada, uno un algoritmo de emparejamiento que genera claves de emparejamiento por separado, de modo que la interfaz aérea no es necesaria para un intercambio de claves de emparejamiento.

2. El método de generación de claves de la reivindicación 1, donde la provisión comprende preconfigurar el primer dispositivo (12) y el segundo dispositivo (14) con la credencial y la función resumen.

3. El método de generación de claves de la reivindicación 1, en el que la credencial es una clave secreta predefinida de 128 bits.

4. El método de generación de claves de la reivindicación 1, en el que las señales de anuncio se generan y transmiten de acuerdo con especificaciones de Bluetooth de baja energía, BLE.

5. El método de generación de claves de la reivindicación 1, en el que la función resumen es un algoritmo resumen seguro seleccionado del grupo que consiste en AES-128 o SHA-256.

6. El método de generación de claves de la reivindicación 1, en el que los datos compartidos son únicos para el primer dispositivo (12) y comprenden al menos un control de acceso al medio, una dirección MAC y un parámetro único dinámico.

7. El método de generación de claves de la reivindicación 1, en el que la clave es una clave fuera de banda, OOB, de 128 bits.

8. El método de generación de claves de la reivindicación 1, en el que el segundo dispositivo (14) y el primer dispositivo (12) realizan emparejamiento OOB entre sí usando su respectiva clave OOB antes de realizar emparejamiento del protocolo de administrador de seguridad, SMP, estándar de Bluetooth de baja energía, BLE, con cálculo de clave de Diffie-Hellman, DH.

9. Un dispositivo (12) para emparejar de forma segura con un segundo dispositivo (14) para comunicación inalámbrica entre ambos, estando el dispositivo provisto inicialmente de una credencial y una función resumen, y comprendiendo:

un dispositivo de memoria configurado para almacenar la credencial y la función resumen;
una interfaz de radiofrecuencia, RF, para transmitir y recibir señales RF a través de al menos una antena; y
un controlador configurado para transmitir señales de anuncio a intervalos seleccionados y en un rango de radiofrecuencia seleccionado a través de la interfaz RF y la antena, comprendiendo las señales de anuncio datos a compartir con un segundo dispositivo (14);
**caracterizado por que** el controlador está configurado además para introducir los datos compartidos y la credencial en la función resumen para generar una clave fuera de banda, OOB, siendo la clave OOB generada por el dispositivo (12) idéntica a una clave OOB generada por el segundo dispositivo (14) cuando este busca y recibe del dispositivo las señales de anuncio con los datos compartidos, y para realizar emparejamiento OOB con el segundo dispositivo (14) utilizando su respectiva clave OOB antes de realizar emparejamiento estándar Bluetooth de baja energía, BLE, en el que se realiza por separado un algoritmo de emparejamiento que genera claves de emparejamiento, de modo que la interfaz aérea no es necesaria para un intercambio de claves de emparejamiento.

10. Un segundo dispositivo (14) para un emparejamiento seguro con un primer dispositivo (12) para comunicación inalámbrica entre ambos, estando previsto inicialmente el dispositivo de una credencial y una función resumen, y comprendiendo:

un dispositivo de memoria configurado para almacenar la credencial y la función resumen;
una interfaz de radiofrecuencia (RF) para transmitir y recibir señales de RF a través de al menos una antena; y
un controlador configurado para
escanear y recibir, a través de la interfaz RF y la antena, señales de anuncio que son transmitidas por un primer dispositivo (12)
a intervalos seleccionados y en un rango de radiofrecuencia seleccionado, comprendiendo las señales de anuncio datos del primer dispositivo (12) a compartir con el dispositivo;
**caracterizado por que** el controlador está configurado además para introducir los datos compartidos y la credencial en la función resumen para generar una clave fuera de banda, OOB, siendo la clave OOB generada por el dispositivo idéntica a una clave OOB generada por el primer dispositivo (12), y
para realizar emparejamiento OOB con el primer dispositivo (12) usando su clave OOB respectiva antes de realizar emparejamiento estándar Bluetooth de baja energía, BLE, en el que se realiza por separado un algoritmo de emparejamiento que genera claves de emparejamiento, de modo que la interfaz aérea no es necesaria para un intercambio de claves de emparejamiento.

11. El dispositivo 2 (12, 14) de la reivindicación 9 ó 10, en el que el primer dispositivo (12) y el segundo dispositivo (14) están preconfigurados con la credencial y la función resumen.

12. El dispositivo (12, 14) de la reivindicación 9 ó 10, en el que la credencial es una clave secreta predefinida de 128 bits.

13. El dispositivo (12, 14) de la reivindicación 9 ó 10, en el que las señales de anuncio se generan y transmiten de acuerdo con especificaciones Bluetooth de baja energía, BLE.

14. El dispositivo (12, 14) de la reivindicación 9 ó 10, en el que la función resumen es un algoritmo resumen seguro seleccionado del grupo que consiste en AES-128 o SHA-256.

15. El dispositivo (12) de la reivindicación 9, en el que los datos compartidos son únicos para el dispositivo y comprenden al menos una dirección de control de acceso al medio, MAC, y un parámetro único dinámico.

16. El dispositivo (14) de la reivindicación 10, en el que los datos compartidos son únicos para el segundo dispositivo y comprenden al menos una dirección de control de acceso al medio, MAC, y un parámetro único dinámico.

17. El dispositivo (12, 14) de la reivindicación 9 ó 10, en el que la clave es una clave fuera de banda, OOB, de 128 bits.

18. El dispositivo (12, 14) de la reivindicación 9 o 10, en el que el segundo dispositivo (14) y el primer dispositivo (12) están configurados para realizar emparejamiento OOB entre sí usando su respectiva clave OOB antes de realizar emparejamiento del protocolo de administrador de seguridad, SMP, estándar de Bluetooth de baja energía, BLE, con cálculo de clave de Diffie-Hellman, DH.

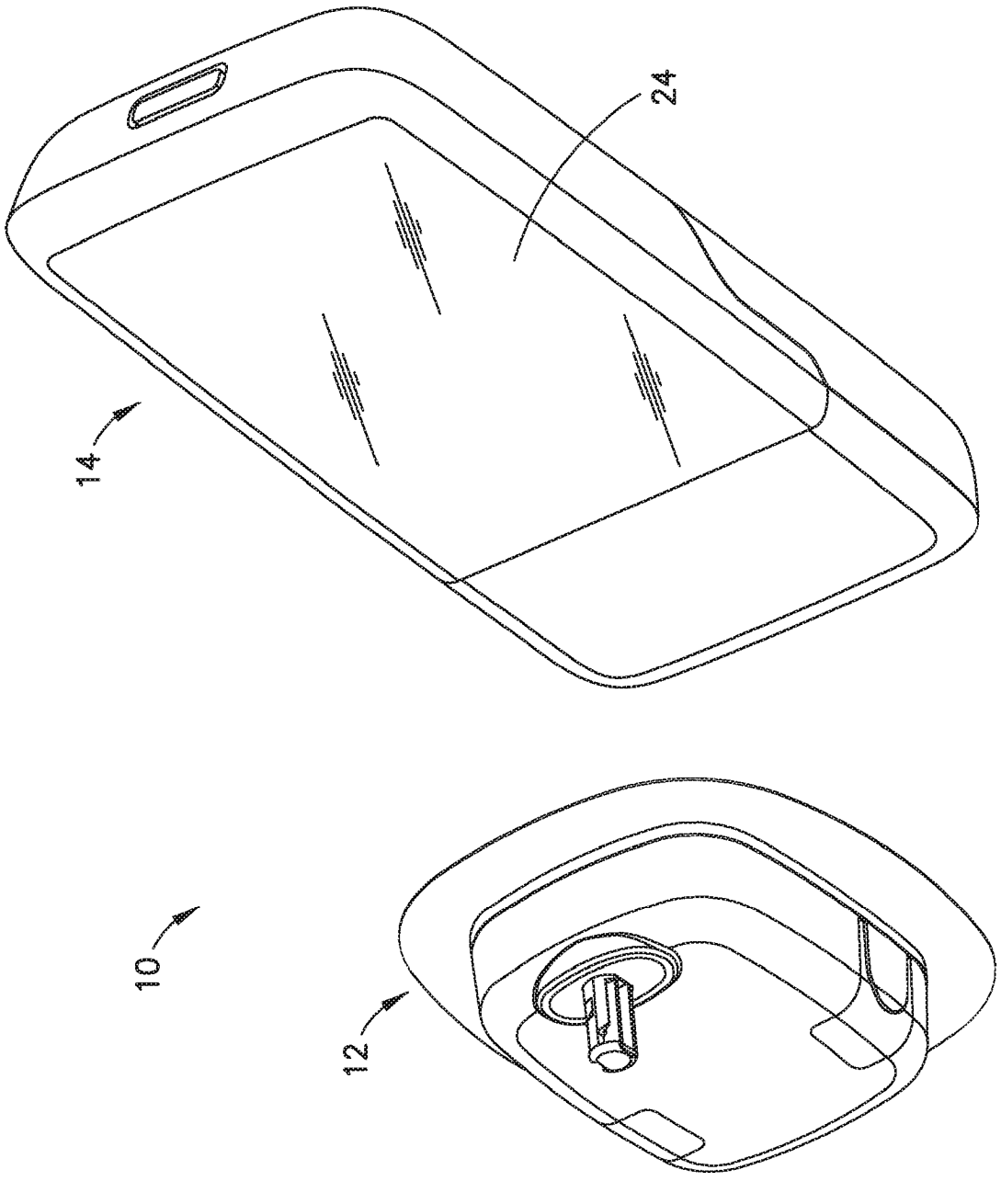


FIG.1

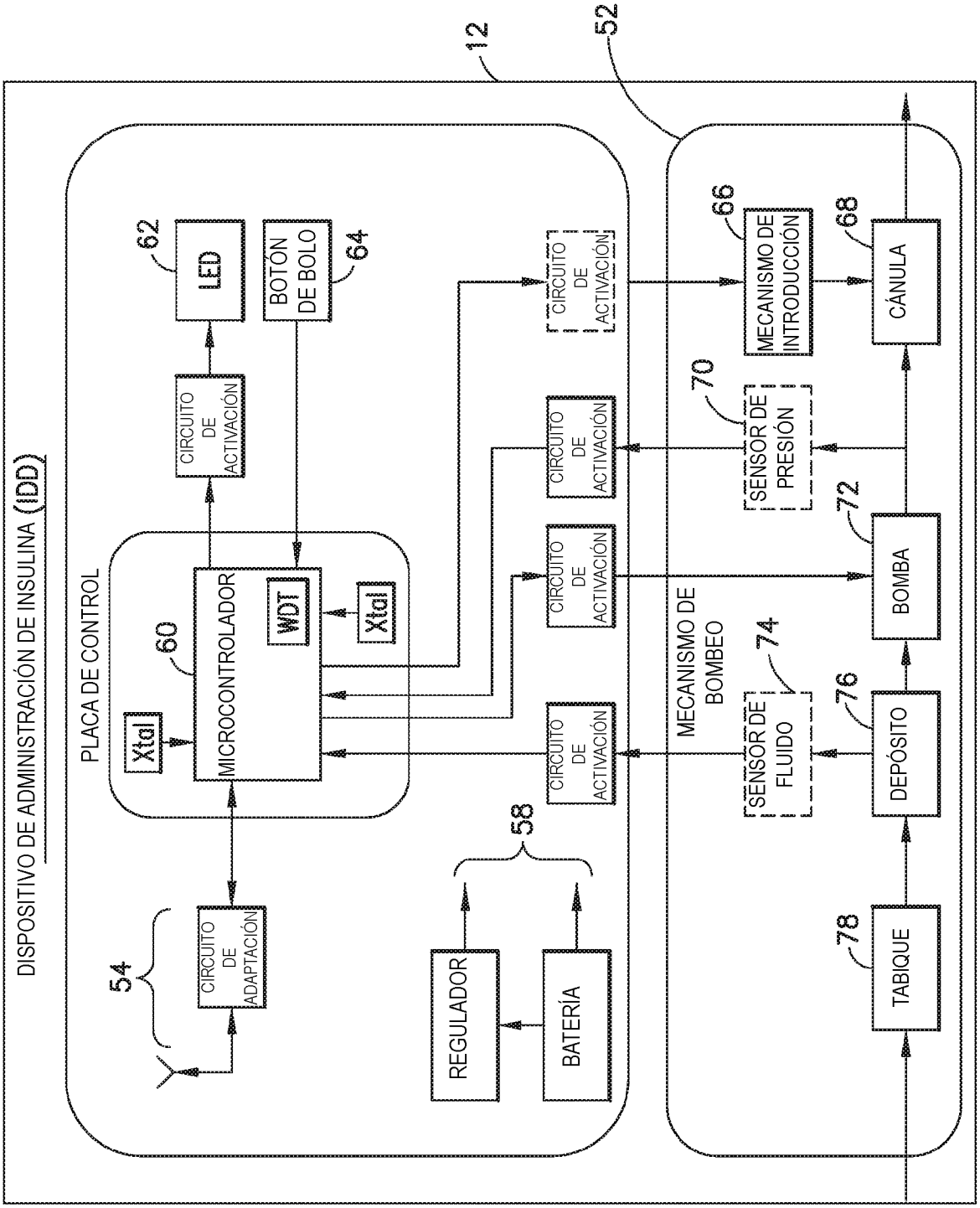
DISPOSITIVO DE ADMINISTRACIÓN DE INSULINA (IDD)
12
52
PLACA DE CONTROL
MECANISMO DE BOMBEO
MICROCONTROLADOR
60
Xtal
WDT
Xtal
LED
62
BOTÓN DE BOLO
64
CIRCUITO DE ACTIVACIÓN
CIRCUITO DE ADAPTACIÓN
54
REGULADOR
BATERÍA
58
MECANISMO DE INTRODUCCIÓN
66
CÁNULA
68
SENSOR DE PRESIÓN
70
BOMBA
72
SENSOR DE FLUIDO
74
DEPÓSITO
76
TABIQUE
78

FIG.2A

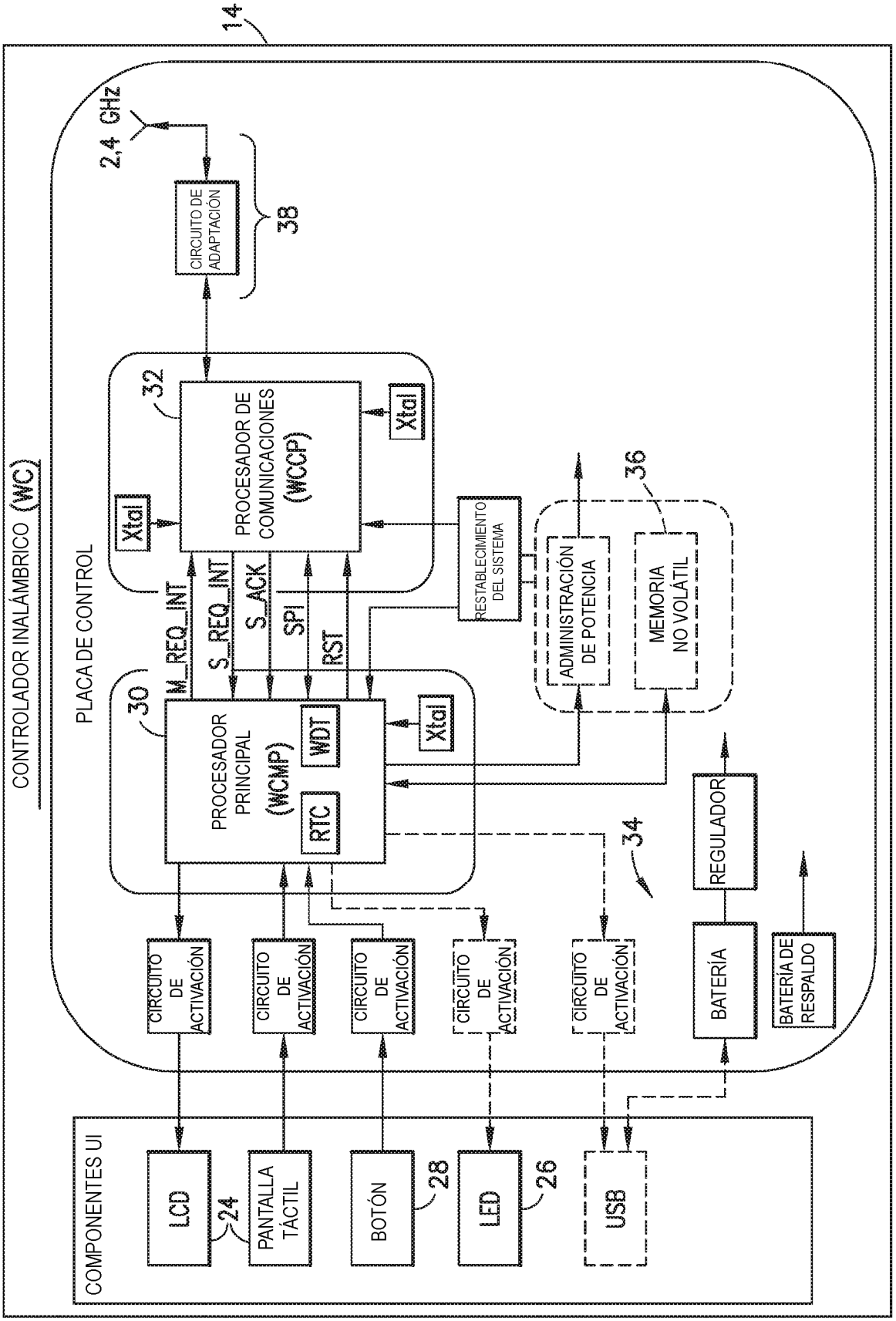
14
CONTROLADOR INALÁMBRICO (WC)
PLACA DE CONTROL
2,4 GHz
CIRCUITO DE ADAPTACIÓN
38
32
PROCESADOR DE COMUNICACIONES (WCCP)
Xtal
Xtal
M_REQ_INT
S_REQ_INT
S_ACK
SPI
RST
RESTABLECIMIENTO DEL SISTEMA
36
ADMINISTRACIÓN DE POTENCIA
MEMORIA NO VOLÁTIL
30
PROCESADOR PRINCIPAL (WCMP)
WDT
RTC
Xtal
34
REGULADOR
BATERÍA
BATERÍA DE RESPALDO
CIRCUITO DE ACTIVACIÓN
CIRCUITO DE ACTIVACIÓN
CIRCUITO DE ACTIVACIÓN
CIRCUITO DE ACTIVACIÓN
CIRCUITO DE ACTIVACIÓN
COMPONENTES UI
LCD
24
PANTALLA TÁCTIL
BOTÓN
28
LED
26
USB

FIG.2B

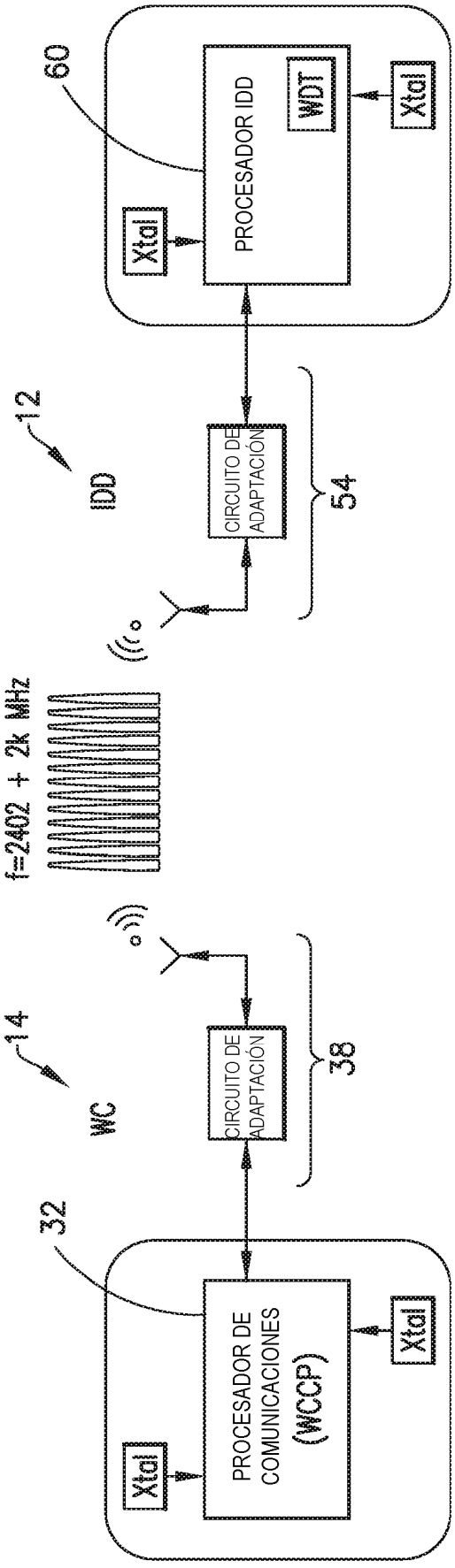
60
PROCESADOR IDD
WDT
Xtal
Xtal
12
IDD
CIRCUITO DE ADAPTACIÓN
54
f=2402 + 2k MHz
14
WC
CIRCUITO DE ADAPTACIÓN
38
32
PROCESADOR DE COMUNICACIONES (WCCP)
Xtal
Xtal

FIG.3

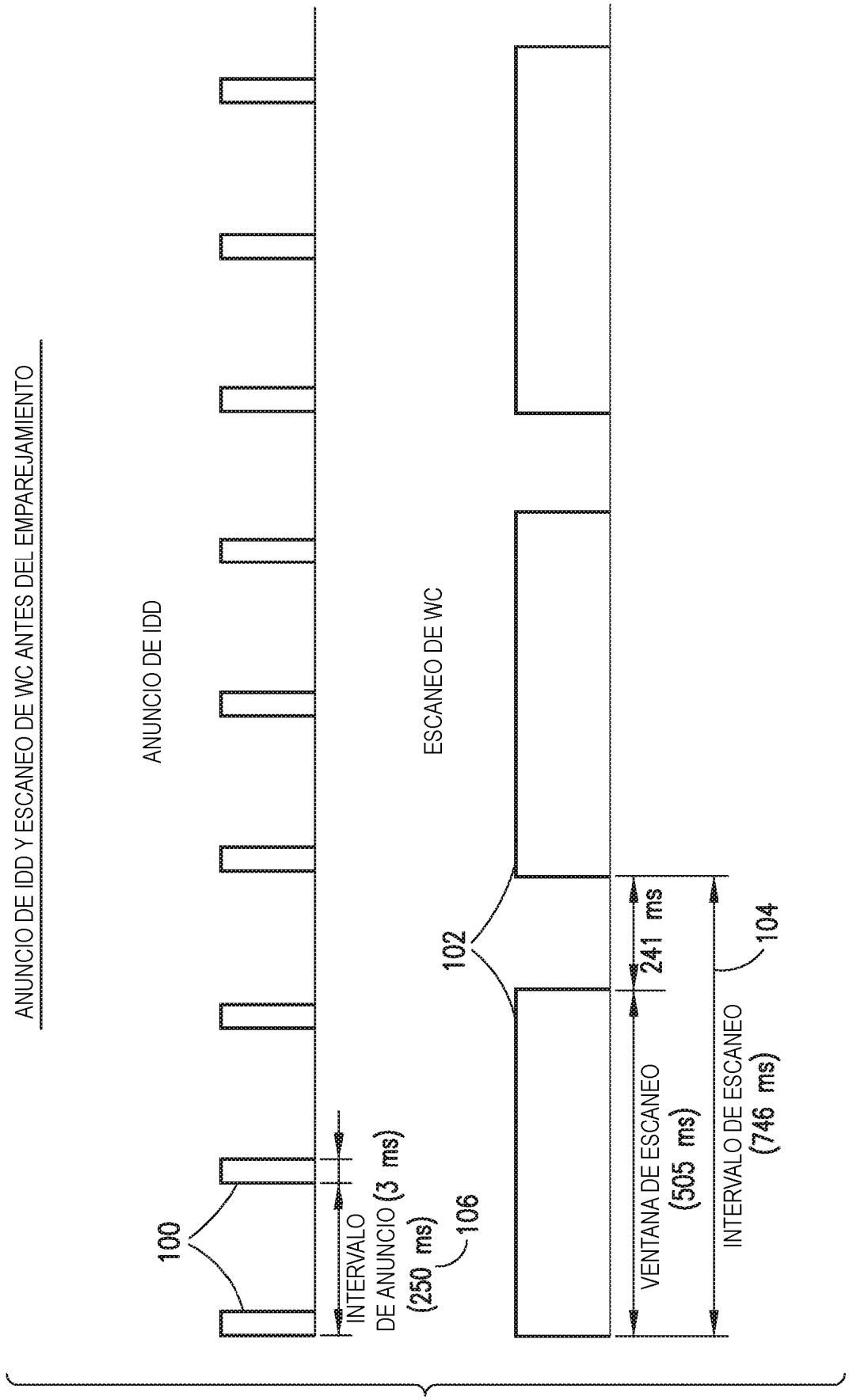
ANUNCIO DE IDD Y ESCANEO DE WC ANTES DEL EMPAREJAMIENTO
ANUNCIO DE IDD
ESCANEO DE WC
100
INTERVALO DE ANUNCIO (3 ms) (250 ms)
106
102
241 ms
VENTANA DE ESCANEO (505 ms)
INTERVALO DE ESCANEO (746 ms)
104

FIG. 4

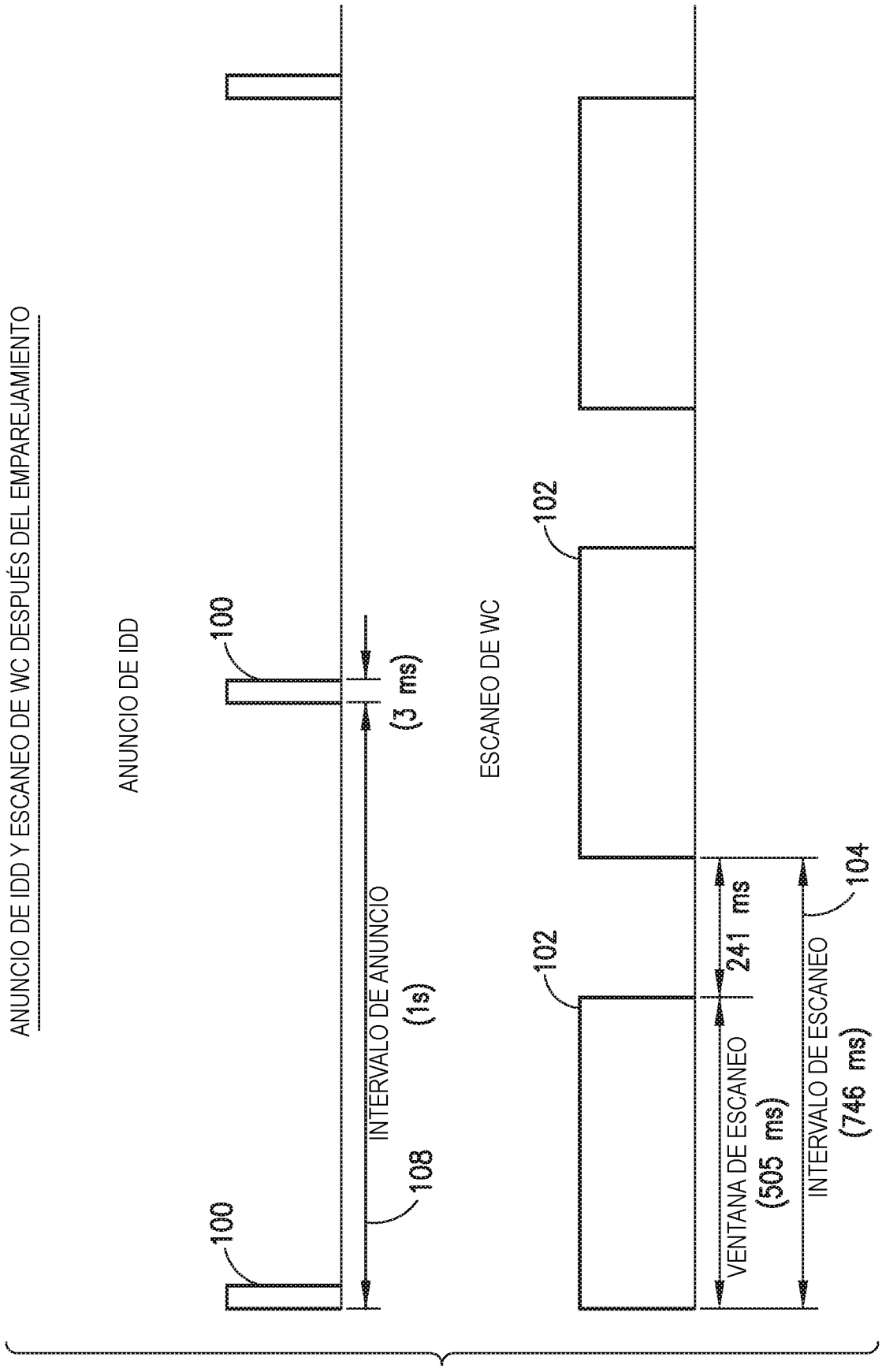
ANUNCIO DE IDD Y ESCANEO DE WC DESPUÉS DEL EMPAREJAMIENTO
ANUNCIO DE IDD
100
100
(3 ms)
INTERVALO DE ANUNCIO
(1s)
108
ESCANEO DE WC
102
102
241 ms
VENTANA DE ESCANEO
(505 ms)
INTERVALO DE ESCANEO
(746 ms)
104

FIG.5

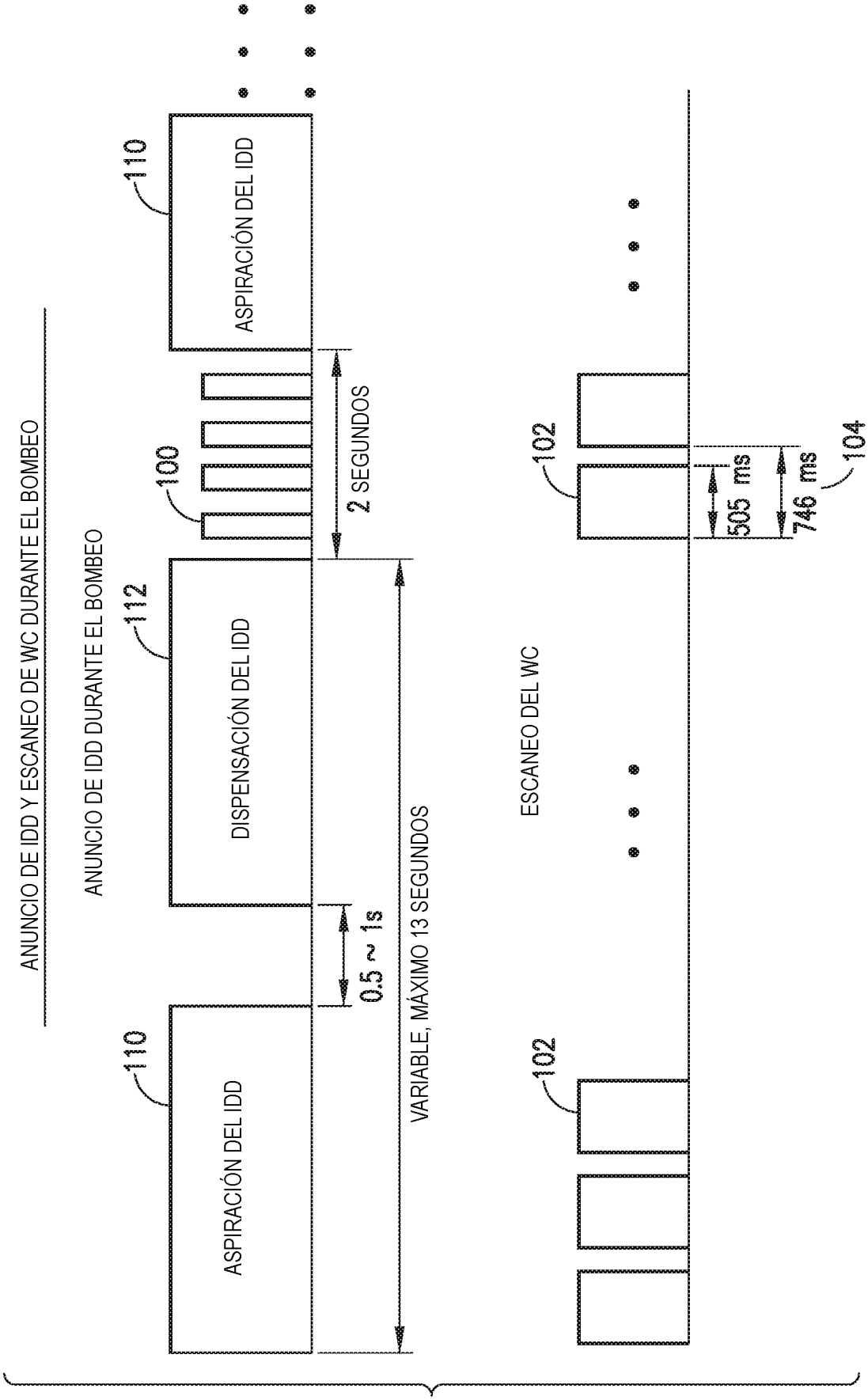
ANUNCIO DE IDD Y ESCANEO DE WC DURANTE EL BOMBEO
ANUNCIO DE IDD DURANTE EL BOMBEO
110
ASPIRACIÓN DEL IDD
112
DISPENSACIÓN DEL IDD
100
2 SEGUNDOS
0.5 ~ 1s
VARIABLE, MÁXIMO 13 SEGUNDOS
ESCANEO DEL WC
102
505 ms
746 ms
104

FIG.6

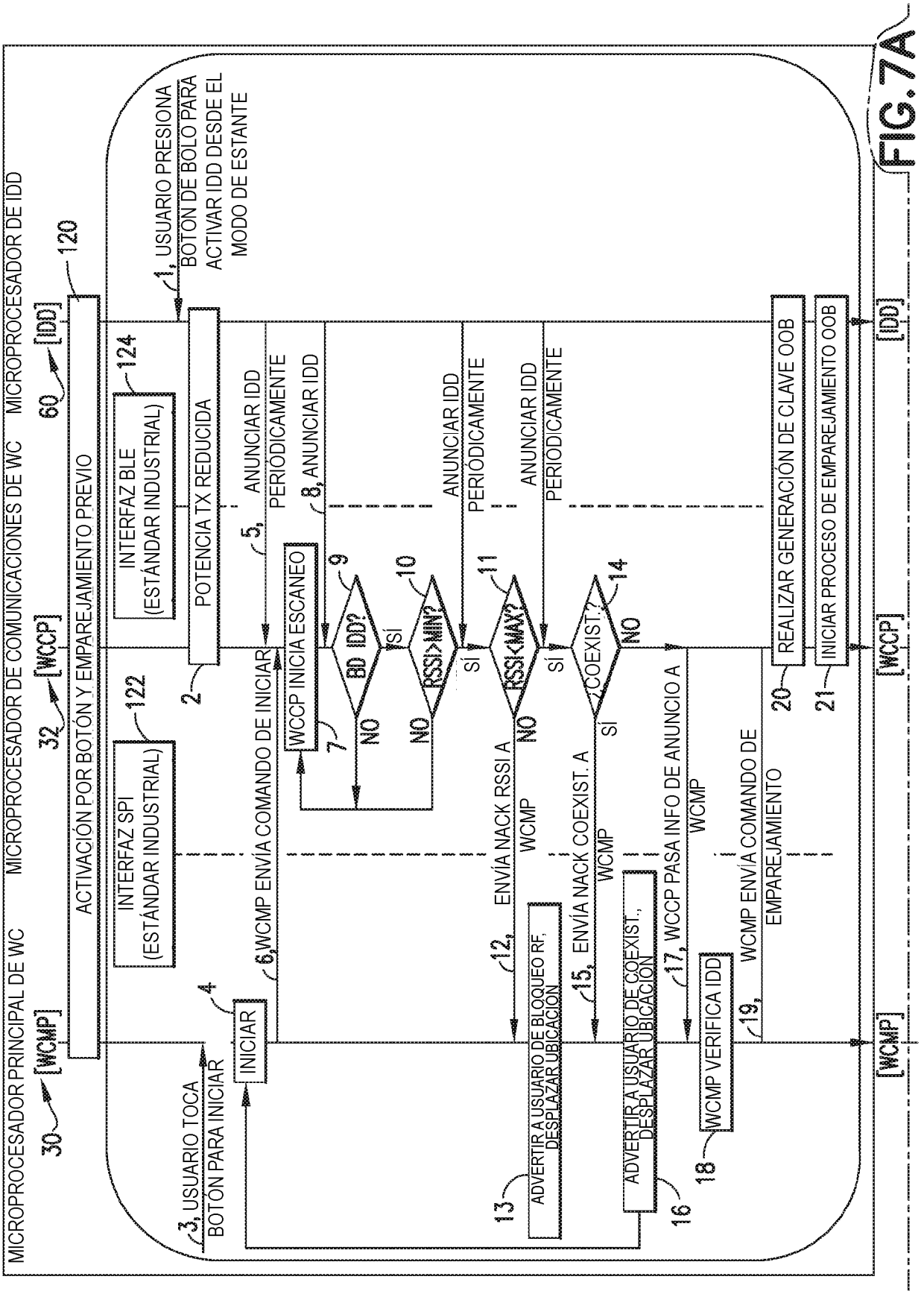
MICROPROCESADOR PRINCIPAL DE WC
MICROPROCESADOR DE COMUNICACIONES DE WC
MICROPROCESADOR DE IDD
[WCMP]
[WCCP]
[IDD]
30
32
60
120
ACTIVACIÓN POR BOTÓN Y EMPAREJAMIENTO PREVIO
INTERFAZ SPI (ESTÁNDAR INDUSTRIAL)
122
INTERFAZ BLE (ESTÁNDAR INDUSTRIAL)
124
1, USUARIO PRESIONA BOTÓN DE BOLO PARA ACTIVAR IDD DESDE EL MODO DE ESTANTE
POTENCIA TX REDUCIDA
2
5, ANUNCIAR IDD PERIÓDICAMENTE
8, ANUNCIAR IDD PERIÓDICAMENTE
ANUNCIAR IDD PERIÓDICAMENTE
ANUNCIAR IDD PERIÓDICAMENTE
3, USUARIO TOCA BOTÓN PARA INICIAR
4
INICIAR
6, WCMP ENVÍA COMANDO DE INICIAR
WCCP INICIA ESCANEO
7
BD IDD?
9
NO
SÍ
RSSI>MIN?
10
NO
SÍ
RSSI<MAX?
11
NO
SÍ
¿COEXIST.?
14
NO
SÍ
12, ENVÍA NACK RSSI A WCMP
13
ADVERTIR A USUARIO DE BLOQUEO RF, DESPLAZAR UBICACIÓN
15, ENVÍA NACK COEXIST. A WCMP
ADVERTIR A USUARIO DE COEXIST., DESPLAZAR UBICACIÓN
16
17, WCCP PASA INFO DE ANUNCIO A WCMP
18
WCMP VERIFICA IDD
19, WCMP ENVÍA COMANDO DE EMPAREJAMIENTO
20
REALIZAR GENERACIÓN DE CLAVE OOB
21
INICIAR PROCESO DE EMPAREJAMIENTO OOB

FIG. 7A

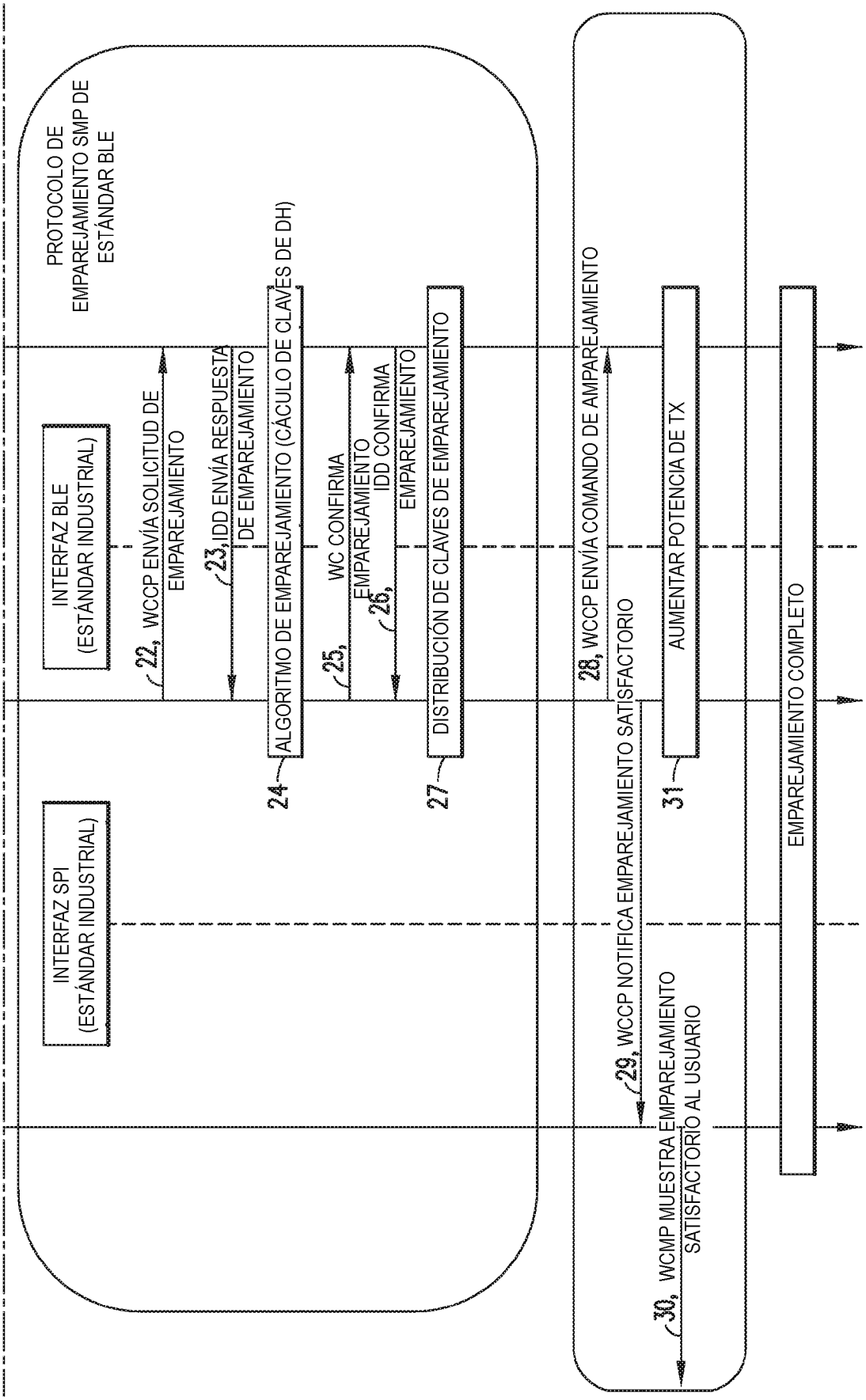


FIG. 7B

FIG. 7

FIG. 7A
FIG. 7B

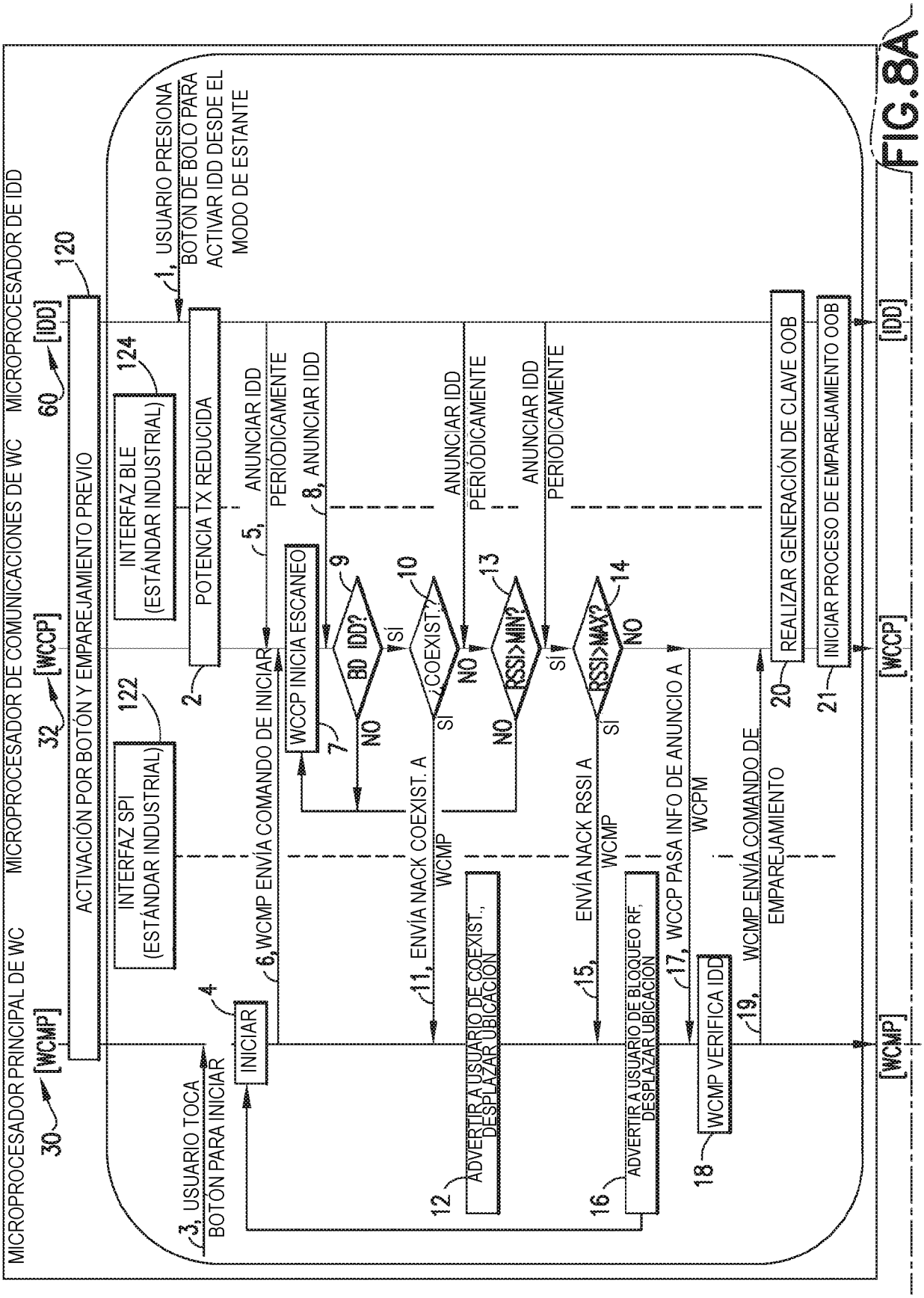
MICROPROCESADOR PRINCIPAL DE WC
MICROPROCESADOR DE COMUNICACIONES DE WC
MICROPROCESADOR DE IDD
[WCMP]
[WCCP]
[IDD]
30
32
60
120
ACTIVACIÓN POR BOTÓN Y EMPAREJAMIENTO PREVIO
INTERFAZ SPI (ESTÁNDAR INDUSTRIAL)
122
INTERFAZ BLE (ESTÁNDAR INDUSTRIAL)
124
1, USUARIO PRESIONA BOTÓN DE BOLO PARA ACTIVAR IDD DESDE EL MODO DE ESTANTE
POTENCIA TX REDUCIDA
2
3, USUARIO TOCA BOTÓN PARA INICIAR
4
INICIAR
6, WCMP ENVÍA COMANDO DE INICIAR
5, ANUNCIAR IDD PERIÓDICAMENTE
WCCP INICIA ESCANEO
7
8, ANUNCIAR IDD
9
BD IDD?
NO
SÍ
10
¿COEXIST.?
SÍ
NO
11, ENVÍA NACK COEXIST. A WCMP
ANUNCIAR IDD PERIÓDICAMENTE
12
ADVERTIR A USUARIO DE COEXIST., DESPLAZAR UBICACIÓN
13
RSSI>MIN?
NO
SÍ
ANUNCIAR IDD PERIÓDICAMENTE
14
RSSI>MAX?
SÍ
NO
15, ENVÍA NACK RSSI A WCMP
16
ADVERTIR A USUARIO DE BLOQUEO RF, DESPLAZAR UBICACIÓN
17, WCCP PASA INFO DE ANUNCIO A WCPM
18
WCMP VERIFICA IDD
19, WCMP ENVÍA COMANDO DE EMPAREJAMIENTO
20
REALIZAR GENERACIÓN DE CLAVE OOB
21
INICIAR PROCESO DE EMPAREJAMIENTO OOB
[WCMP]
[WCCP]
[IDD]

FIG.8A

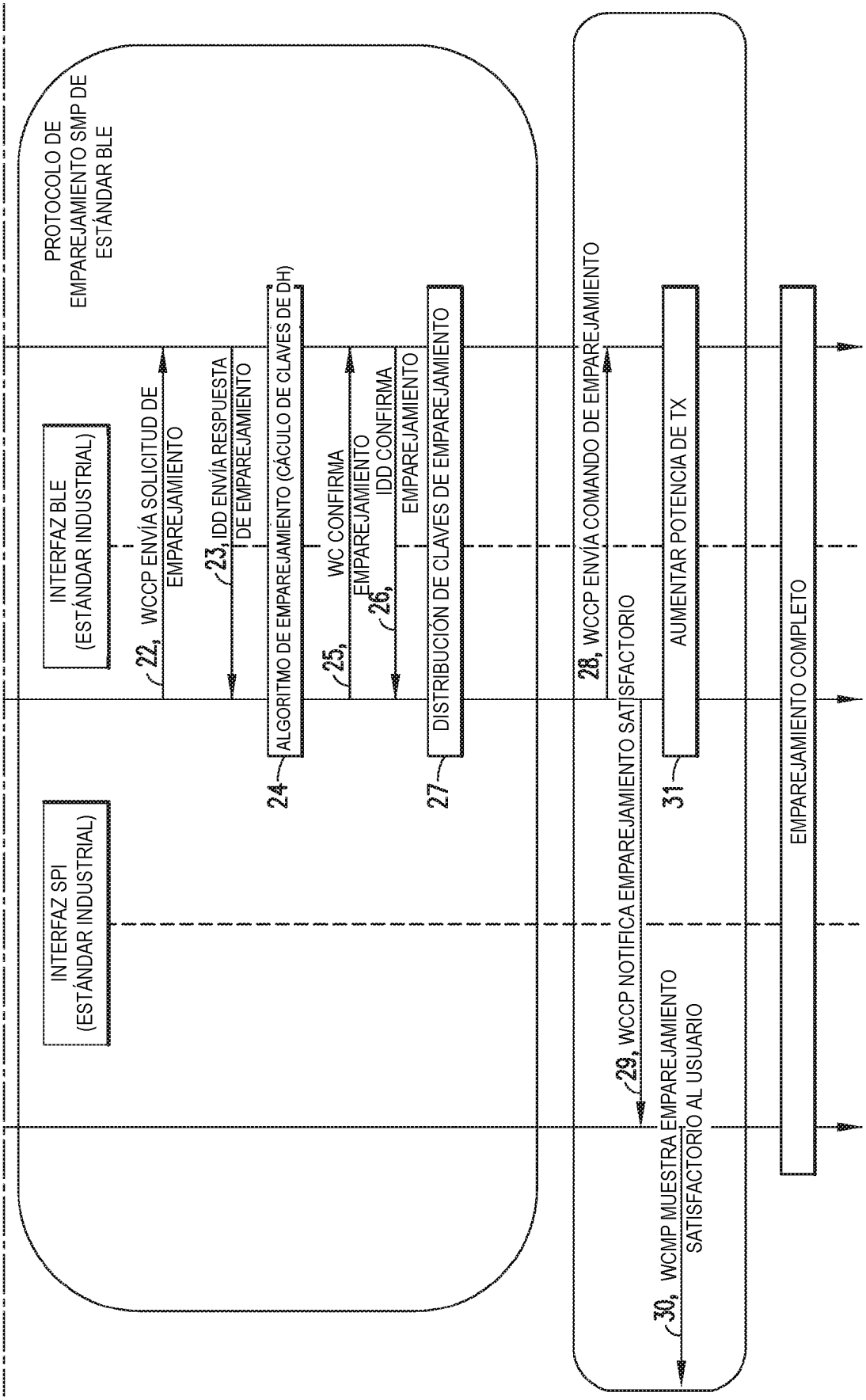


FIG.8B

FIG.8A
FIG.8B

FIG.8

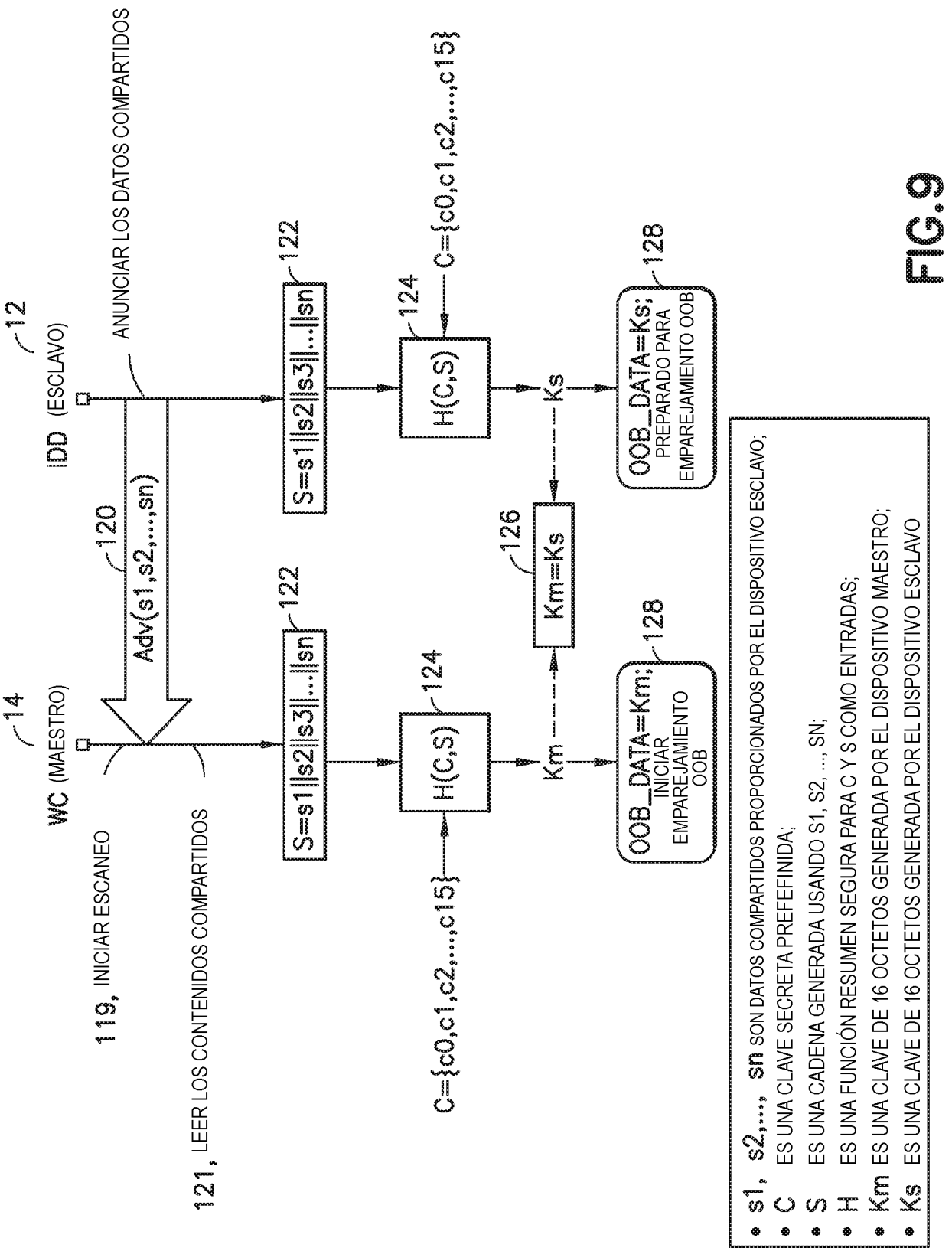
14
WC (MAESTRO)
12
IDD (ESCLAVO)
119, INICIAR ESCANEO
ANUNCIAR LOS DATOS COMPARTIDOS
120
Adv(s1,s2,...,sn)
121, LEER LOS CONTENIDOS COMPARTIDOS
122
S=s1||s2||s3||...||sn
124
H(C,S)
C={c0,c1,c2,...,c15}
126
Km=Ks
Km
Ks
128
OOB_DATA=Km;
INICIAR EMPAREJAMIENTO OOB
OOB_DATA=Ks;
PREPARADO PARA EMPAREJAMIENTO OOB
• s1, s2,..., sn SON DATOS COMPARTIDOS PROPORCIONADOS POR EL DISPOSITIVO ESCLAVO;
• C ES UNA CLAVE SECRETA PREFEFINIDA;
• S ES UNA CADENA GENERADA USANDO S1, S2, ..., SN;
• H ES UNA FUNCIÓN RESUMEN SEGURA PARA C Y S COMO ENTRADAS;
• Km ES UNA CLAVE DE 16 OCTETOS GENERADA POR EL DISPOSITIVO MAESTRO;
• Ks ES UNA CLAVE DE 16 OCTETOS GENERADA POR EL DISPOSITIVO ESCLAVO

FIG.9