(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 930 238**

(51) Int. CI.:

G16H 40/63 (2008.01)
H04W 12/50 (2011.01)
H04W 84/18 (2009.01)
H04W 12/65 (2011.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **07.12.2015 PCT/IB2015/059400**

(87) Fecha y número de publicación internacional: **16.06.2016 WO16092448**

(96) Fecha de presentación y número de la solicitud europea: **07.12.2015 E 15867171 (9)**

(97) Fecha y número de publicación de la concesión europea: **14.09.2022 EP 3230909**

(54) Título: **Emparejamiento de un aparato médico con una unidad de control**

(30) Prioridad:

08.12.2014 EP 14196797

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
09.12.2022

(73) Titular/es:

ROCHE DIABETES CARE GMBH (50.0%)
Sandhofer Straße 116
68305 Mannheim, DE y
F. HOFFMANN-LA ROCHE AG (50.0%)

(72) Inventor/es:

HECK, WOLFGANG;
SCHWENKER, KAI-OLIVER;
SCHMITZ, RALF;
ZEUNER, VOLKER;
MUEGLITZ, CARSTEN;
EISSENLOEFFEL, THOMAS y
LUSZICK, CHRISTIAN-ALEXANDER

(74) Agente/Representante:

LINAGE GONZÁLEZ, Rafael

DESCRIPCIÓN

Emparejamiento de un aparato médico con una unidad de control

Campo de la invención

La invención se refiere a instrumentos médicos para supervisar y mantener el nivel de glucemia de un sujeto.

Antecedentes y técnica relacionada

Las denominadas bombas de insulina de parche y glucómetros se fijan a la superficie de un sujeto. Es ventajoso minimizar el peso de estas bombas y monitores usando una unidad de control que esté separada de la parte fijada al sujeto. Si se realiza una conexión inalámbrica entre la parte fijada al sujeto y la unidad de control, es fundamental que la conexión sea segura e impermeable a los ataques. Perder el control de una bomba de insulina a manos de un pirata informático podría poner en peligro la salud de la persona que lleva la bomba.

Sumario

La invención se refiere a un procedimiento de funcionamiento de un instrumento médico y un instrumento médico en las reivindicaciones independientes. Se dan modos de realización en las reivindicaciones dependientes.

Como se apreciará por un experto en la técnica, los aspectos de la presente invención se pueden incorporar como un aparato, procedimiento o producto de programa informático. En consecuencia, los aspectos de la presente invención pueden adoptar la forma de un modo de realización de equipo informático completamente, un modo de realización de programa informático completamente (incluyendo soporte lógico inalterable, programa informático residente, microcódigo, etc.) o un modo de realización que combine aspectos de programa informático y de equipo informático que en conjunto se pueden denominar en el presente documento, en general, "circuito", "módulo" o "sistema". Además, los aspectos de la presente invención pueden adoptar la forma de un producto de programa informático incorporado en uno o más medios legibles por ordenador que tienen un código ejecutable por ordenador incorporado en los mismos.

Se puede utilizar cualquier combinación de uno o más medios legibles por ordenador. El medio legible por ordenador puede ser un medio de señal legible por ordenador o un medio de almacenamiento legible por ordenador. Un 'medio de almacenamiento legible por ordenador' como se usa en el presente documento engloba cualquier medio de almacenamiento tangible que pueda almacenar instrucciones que sean ejecutables por un procesador de un dispositivo informático. El medio de almacenamiento legible por ordenador se puede denominar medio de almacenamiento no transitorio legible por ordenador. El medio de almacenamiento legible por ordenador también se puede denominar medio legible por ordenador tangible. En algunos modos de realización, un medio de almacenamiento legible por ordenador también puede almacenar datos a los que se puede acceder por el procesador del dispositivo informático. Los ejemplos de medios de almacenamiento legibles por ordenador incluyen, pero no se limitan a: un disquete, un disco duro magnético, un disco duro de estado sólido, memoria rápida, una memoria USB, memoria de acceso aleatorio (RAM), memoria de solo lectura (ROM), un disco óptico, un disco magnetoóptico y el archivo de registro del procesador. Los ejemplos de discos ópticos incluyen discos compactos (CD) y discos versátiles digitales (DVD), por ejemplo, discos CD-ROM, CD-RW, CD-R, DVD-ROM, DVD-RW o DVD-R. El término medio de almacenamiento legible por ordenador también se refiere a diversos tipos de medios de registro a los que se puede acceder por el dispositivo informático por medio de una red o enlace de comunicación. Por ejemplo, se pueden recuperar datos a través de un módem, a través de Internet o a través de una red de área local. Se puede transmitir el código ejecutable por ordenador incorporado en un medio legible por ordenador usando cualquier medio apropiado, incluyendo, pero sin limitarse a inalámbrico, por cable, cable de fibra óptica, RF, etc., o cualquier combinación adecuada de los anteriores.

Un medio de señal legible por ordenador puede incluir una señal de datos propagada con código ejecutable por ordenador incorporado en la misma, por ejemplo, en banda base o como parte de una onda portadora. Una señal propagada de este tipo puede adoptar cualquiera de una variedad de formas, incluyendo, pero sin limitarse a, electromagnética, óptica o cualquier combinación adecuada de las mismas. Un medio de señal legible por ordenador puede ser cualquier medio legible por ordenador que no sea un medio de almacenamiento legible por ordenador y que pueda comunicar, propagar o transportar un programa para su uso por o en conexión con un sistema, aparato o dispositivo de ejecución de instrucciones.

La 'memoria informática' o 'memoria' es un ejemplo de un medio de almacenamiento legible por ordenador. La memoria informática es cualquier memoria que sea directamente accesible a un procesador. El 'almacenamiento informático' o 'almacenamiento' es otro ejemplo de un medio de almacenamiento legible por ordenador. El almacenamiento informático es cualquier medio de almacenamiento legible por ordenador no volátil. En algunos modos de realización, el almacenamiento informático también puede ser la memoria informática o viceversa.

Un 'procesador' como se usa en el presente documento engloba un componente electrónico que puede ejecutar un

programa o instrucción ejecutable por máquina o código ejecutable por ordenador. Las referencias al dispositivo informático que comprende "un procesador" se deben interpretar como que posiblemente contiene más de un procesador o núcleo de procesamiento. El procesador puede ser, por ejemplo, un procesador de múltiples núcleos. Un procesador también se puede referir a un grupo de procesadores dentro de un único sistema informático o distribuidos entre múltiples sistemas informáticos. El término dispositivo informático también se debe interpretar para referirse posiblemente a un grupo o red de dispositivos informáticos, comprendiendo cada uno un procesador o procesadores. El código ejecutable por ordenador se puede ejecutar por múltiples procesadores que pueden estar dentro del mismo dispositivo informático o que incluso pueden estar distribuidos a lo largo de múltiples dispositivos informáticos.

El código ejecutable por ordenador puede comprender instrucciones ejecutables por máquina o un programa que hace que un procesador realice un aspecto de la presente invención. El código ejecutable por ordenador para llevar a cabo operaciones para aspectos de la presente invención se puede escribir en cualquier combinación de uno o más lenguajes de programación, incluyendo un lenguaje de programación orientado a objetos, tal como Java, Smalltalk, C++ o similares y lenguajes de programación por procedimientos convencionales, tales como el lenguaje de programación "C" o lenguajes de programación similares, y compilar en instrucciones ejecutables por máquina. En algunos casos, el código ejecutable por ordenador puede estar en forma de un lenguaje de nivel alto o en una forma precompilada y usarse junto con un intérprete que genera las instrucciones ejecutables por máquina sobre la marcha.

El código ejecutable por ordenador se puede ejecutar completamente en el ordenador del usuario, en parte en el ordenador del usuario, como un paquete de programa informático independiente, en parte en el ordenador del usuario y en parte en un ordenador remoto o completamente en el ordenador o servidor remoto. En la última situación, el ordenador remoto se puede conectar al ordenador del usuario a través de cualquier tipo de red, incluyendo una red de área local (LAN) o una red de área amplia (WAN), o se puede establecer la conexión a un ordenador externo (por ejemplo, a través de Internet usando un proveedor de acceso de Internet).

Se describen aspectos de la presente invención con referencia a diagramas de flujo, ilustraciones y/o diagramas de bloques de procedimientos, aparatos (sistemas) y productos de programa informático de acuerdo con modos de realización de la invención. Se entenderá que cada bloque o una parte de los bloques del diagrama de flujo, ilustraciones y/o diagramas de bloques se puede implementar por instrucciones de programa informático en forma de código ejecutable por ordenador cuando sea aplicable. Se entiende además que, cuando no sean mutuamente excluyentes, se pueden combinar combinaciones de bloques en diferentes diagramas de flujo, ilustraciones y/o diagramas de bloques. Se pueden proporcionar estas instrucciones de programa informático a un procesador de un ordenador de propósito general, ordenador de propósito especial u otro aparato de procesamiento de datos programable para producir una máquina, de modo que las instrucciones, que se ejecutan por medio del procesador del ordenador u otro aparato de procesamiento de datos programable, creen medios para implementar las funciones/acciones especificadas en el diagrama de flujo y/o bloque o bloques del diagrama de bloques.

También se pueden almacenar estas instrucciones de programa informático en un medio legible por ordenador que pueda dirigir un ordenador, otro aparato de procesamiento de datos programable u otros dispositivos para que funcionen de una manera particular, de modo que las instrucciones almacenadas en el medio legible por ordenador produzcan un artículo de fabricación, incluyendo instrucciones que implementan la función/acción especificada en el diagrama de flujo y/o bloque o bloques del diagrama de bloques.

También se pueden cargar las instrucciones de programa informático en un ordenador, otro aparato de procesamiento de datos programable u otros dispositivos para provocar que se realice una serie de etapas operativas en el ordenador, otro aparato programable u otros dispositivos para producir un procedimiento implementado por ordenador, de modo que las instrucciones que se ejecutan en el ordenador u otro aparato programable proporcionan procedimientos para implementar las funciones/acciones especificadas en el diagrama de flujo y/o bloque o bloques del diagrama de bloques.

Una 'interfaz de usuario' como se usa en el presente documento es una interfaz que permite que un usuario u operario interactúe con un ordenador o sistema informático. Una 'interfaz de usuario' también se puede denominar 'dispositivo de interfaz humana'. Una interfaz de usuario puede proporcionar información o datos al operario y/o recibir información o datos del operario. Una interfaz de usuario puede posibilitar que la entrada de un operario se reciba por el ordenador y puede proporcionar salida al usuario desde el ordenador. En otras palabras, la interfaz de usuario puede permitir que un operario controle o manipule un ordenador y la interfaz puede permitir que el ordenador indique los efectos del control o manipulación del operario. La visualización de datos o información en una pantalla o una interfaz gráfica de usuario es un ejemplo de proporcionar información a un operario. La recepción de datos a través de un teclado, ratón, bola de desplazamiento, panel táctil, pantalla táctil, dispositivo de puntero, tableta gráfica, palanca de mando, controlador de videojuego, cámara web, auriculares, palancas de cambios, volante, pedales, guantes con cable, almohadilla de baile, control remoto y acelerómetro son todos ejemplos de componentes de interfaz de usuario que posibilitan la recepción de información o datos de un operario.

Una 'interfaz de equipo informático' como se usa en el presente documento engloba una interfaz que posibilita que

el procesador de un sistema informático interactúe con y/o controle un dispositivo y/o aparato informático externo. Una interfaz de equipo informático puede permitir que un procesador envíe señales de control o instrucciones a un dispositivo y/o aparato informático externo. Una interfaz de equipo informático también puede posibilitar que un procesador intercambie datos con un dispositivo y/o aparato informático externo. Los ejemplos de una interfaz de equipo informático incluyen, pero no se limitan a: un bus serie universal, puerto IEEE 1394, puerto paralelo, puerto IEEE 1284, puerto serie, puerto RS-232, puerto IEEE-488, conexión Bluetooth, conexión de red inalámbrica de área local, conexión por Ethernet, interfaz de tensión de control, interfaz MIDI, interfaz de entrada analógica e interfaz de entrada digital.

Una 'pantalla' o 'dispositivo de pantalla' como se usa en el presente documento engloba un dispositivo de salida o una interfaz de usuario adaptada para visualizar imágenes o datos. Una pantalla puede emitir datos visuales, de audio o táctiles. Los ejemplos de una pantalla incluyen, pero no se limitan a: un monitor de ordenador, una pantalla de televisión, una pantalla táctil, pantalla electrónica táctil, pantalla Braille, tubo de rayos catódicos (CRT), tubo de almacenamiento, pantalla biestable, tinta electrónica, monitor vectorial, pantalla plana, pantalla fluorescente de vacío (VF), pantallas de diodos emisores de luz (LED), pantalla electroluminiscente (ELD), pantalla de plasma (PDP), pantalla de cristal líquido (LCD), pantallas de diodos emisores de luz orgánicos (OLED), un proyector y casco de realidad virtual.

En un aspecto, la invención se refiere a un procedimiento de funcionamiento de un instrumento médico. El instrumento médico comprende un aparato eléctrico médico y una unidad de control. El aparato eléctrico médico está alimentado por una primera pila. La unidad de control está alimentada por una segunda pila. El aparato eléctrico médico comprende una parte electrónica y una parte subcutánea. La parte subcutánea puede incluir cosas tales como una cánula para fijar a una bomba para bombear un líquido a un sujeto. La parte subcutánea también puede incluir un sensor que se puede insertar en un sujeto. La parte electrónica comprende un primer procesador y una primera memoria. La primera memoria contiene una contraseña de un solo uso.

Una contraseña de un solo uso engloba una contraseña que se puede usar o está destinada a usarse una sola vez. Se evita que la contraseña de un solo uso almacenada en la primera memoria se use de nuevo después de que la clave de cifrado de Bluetooth se almacene en la primera memoria, porque el algoritmo de concordancia de clave autenticada por contraseña está desactivado. En este contexto, la contraseña de un solo uso significa que la contraseña de un solo uso solo se puede usar una vez para emparejar el dispositivo médico. Por lo tanto, se considera que el término un solo uso es descriptivo de cómo se usa la contraseña. El término "contraseña de un solo uso" se puede considerar equivalente y/o con el término "contraseña de un único uso" o "contraseña" en el presente documento.

La primera memoria comprende además una implementación de un algoritmo de concordancia de clave autenticada por contraseña.

La implementación del algoritmo de concordancia de clave autenticada por contraseña se puede ejecutar o está en forma de instrucciones ejecutables por máquina para su ejecución por el primer procesador.

La unidad de control comprende un segundo procesador y una segunda memoria. La unidad de control comprende una interfaz de entrada de datos. La segunda memoria contiene la implementación del algoritmo de concordancia de clave autenticada por contraseña. La implementación del algoritmo de concordancia de clave autenticada por contraseña en la segunda memoria está en forma ejecutable por máquina para su ejecución por el segundo procesador. El algoritmo de concordancia de clave autenticada por contraseña en la primera y segunda memoria es complementario. En otras palabras, la implementación del algoritmo de concordancia de clave autenticada por contraseña en la primera memoria es una primera parte del algoritmo. La implementación del algoritmo de concordancia de clave autenticada por contraseña en la segunda memoria es una segunda parte del algoritmo de concordancia de clave autenticada por contraseña. Las primera y segunda partes del algoritmo de concordancia de clave autenticada por contraseña funcionan conjuntamente de modo que el primer procesador y el segundo procesador ejecutan el algoritmo de concordancia de clave autenticada por contraseña entre sí.

El aparato eléctrico médico comprende un primer módulo de comunicación Bluetooth. La unidad de control comprende además un segundo módulo de comunicación Bluetooth. El primer módulo de comunicación Bluetooth y el segundo módulo de comunicación Bluetooth son operativos para formar un canal de comunicación inalámbrica entre el aparato médico y la unidad de control.

El procedimiento comprende la etapa de introducir la contraseña de un solo uso en la interfaz de entrada de datos. Esta etapa puede adoptar diferentes formas. Por ejemplo, si la interfaz de entrada de datos es un teclado, un usuario puede simplemente escribir la contraseña de un solo uso en la interfaz de entrada de datos. En otros ejemplos, la interfaz de entrada de datos puede ser una variedad de otros tipos de interfaces o lectores para recibir datos. Por ejemplo, la interfaz de entrada de datos puede comprender un sistema óptico, acústico o de radiofrecuencia para recibir la contraseña de un solo uso.

El procedimiento comprende además la etapa de generar una clave de cifrado de Bluetooth por el aparato eléctrico

médico y la unidad de control con la contraseña de un solo uso intercambiando datos a través del canal de comunicación inalámbrica ejecutando el algoritmo de concordancia de clave autenticada por contraseña. La unidad de control inicia la ejecución del algoritmo de concordancia de clave autenticada por contraseña. La contraseña de un solo uso se usa como un secreto compartido por el algoritmo de concordancia de clave autenticada por contraseña para generar la clave de cifrado de Bluetooth. El uso de la contraseña de un solo uso como secreto compartido evita los denominados ataques de intermediarios.

El procedimiento comprende además la etapa de almacenar la clave de cifrado de Bluetooth en la primera memoria. El procedimiento comprende además la etapa de desactivar el algoritmo de concordancia de clave autenticada por contraseña en la primera memoria después de almacenar la clave de cifrado de Bluetooth en la primera memoria. Una vez que el algoritmo de concordancia de clave autenticada por contraseña se ha ejecutado una vez para generar la clave de cifrado de Bluetooth, el instrumento médico ya no puede ejecutar el algoritmo de concordancia de clave autenticada por contraseña. Esto evita que el aparato eléctrico médico se empareje con cualquier otro dispositivo excepto la unidad de control. El procedimiento comprende además la etapa de almacenar la clave de cifrado de Bluetooth en la segunda memoria. El procedimiento comprende además la etapa de establecer un canal de comunicación Bluetooth cifrado usando el primer módulo de comunicación Bluetooth y un segundo módulo de comunicación Bluetooth. El canal de comunicación Bluetooth cifrado se cifra usando la clave de cifrado de Bluetooth.

Al usar la contraseña de un solo uso como un secreto compartido, se puede usar el algoritmo de concordancia de clave autenticada por contraseña por el instrumento médico y la unidad de control para establecer una clave de cifrado de Bluetooth de forma segura. El secreto compartido se comparte fuera del canal de comunicación inalámbrica formado por los módulos de comunicación Bluetooth. Esto puede incrementar en gran medida la seguridad y reducir el riesgo de que el aparato eléctrico médico se pueda interceptar o controlar por algo que no sea la unidad de control.

Puesto que el aparato eléctrico médico está desactivado para repetir el algoritmo de concordancia de clave autenticada por contraseña, el emparejamiento del aparato eléctrico médico con una unidad de control solo puede ocurrir una vez. Si el aparato eléctrico médico y la unidad de control pierden la conexión, se pueden volver a emparejar usando de nuevo la clave de cifrado de Bluetooth.

En otro modo de realización, el algoritmo de concordancia de clave autenticada por contraseña es un algoritmo J-PAKE. El algoritmo J-PAKE también se puede denominar en el presente documento algoritmo de concordancia de clave autenticada por contraseña. Un algoritmo o protocolo J-PAKE es un tipo de protocolo de concordancia de clave autenticado por contraseña que posibilita que dos partes establezcan una comunicación privada y autenticada únicamente en base a su contraseña compartida (baja entropía) sin requerir el uso de una infraestructura de clave pública. El uso de un algoritmo J-PAKE proporciona seguridad adicional y elimina la posibilidad de un ataque de un intermediario sin una infraestructura de clave pública complicada.

Algunos modos de realización pueden proporcionar una seguridad mejorada del emparejamiento entre el aparato eléctrico médico y la unidad de control. En particular, la combinación de usar un algoritmo J-PAKE para emparejar y a continuación desactivar el algoritmo J-PAKE en la primera memoria hace que la contraseña de un solo uso sea funcional para emparejar solo una vez sin el uso de un servidor o sistema externo para gestionar claves. El uso del algoritmo J-PAKE también evita cualquier tipo de ataque de intermediarios.

En otro modo de realización, la parte subcutánea comprende un sensor de glucosa (130). El aparato eléctrico médico comprende un sistema de supervisión continua de glucosa (126, 130). El procedimiento comprende la etapa de registrar una medición de glucosa usando el sistema de supervisión continua de glucosa. El procedimiento comprende además la etapa de transferir la medición de glucosa a la unidad de control usando el canal de comunicación Bluetooth cifrado.

En otro modo de realización, la parte subcutánea comprende al menos una cánula (124). El aparato eléctrico médico comprende un sistema de bombeo (122). El sistema de bombeo comprende una cualquiera de las siguientes: una bomba de insulina para bombear insulina a través de la al menos una cánula, una bomba de glucagón para bombear glucagón a través de la al menos una cánula y combinaciones de las mismas. El procedimiento comprende además la etapa de controlar el sistema de bombeo por medio del canal de comunicación Bluetooth cifrado por la unidad de control.

En otro modo de realización, el algoritmo de concordancia de clave autenticada por contraseña es un algoritmo J-PAKE.

En otro modo de realización, la desactivación del algoritmo de concordancia de clave autenticada por contraseña en la primera memoria comprende evitar la ejecución del algoritmo de concordancia de clave autenticada por contraseña por el primer procesador después de que se ha almacenado la clave de cifrado de Bluetooth en la primera memoria.

En algunos ejemplos, esto se podría lograr, por ejemplo, por primeras instrucciones ejecutables por máquina en la primera memoria que contengan comandos que eviten la ejecución del algoritmo de concordancia de clave autenticada por contraseña después de que se almacene la clave de cifrado de Bluetooth en la primera memoria. Estas primeras instrucciones de la máquina o incluso la implementación del propio algoritmo de concordancia de clave autenticada por contraseña se podrían modificar de modo que se elimine o sobrescriba todo o una parte del algoritmo de concordancia de clave autenticada por contraseña en la primera memoria. Esto haría imposible inducir al aparato eléctrico médico a pasar por el procedimiento de emparejamiento de Bluetooth por segunda vez, incluso si el dispositivo se pirateara.

En otro modo de realización, la desactivación del algoritmo J-PAKE en la primera memoria comprende evitar la ejecución del algoritmo J-PAKE por el primer procesador después de que se ha almacenado la clave de cifrado de Bluetooth en la primera memoria.

En algunos ejemplos, esto se podría lograr, por ejemplo, por primeras instrucciones ejecutables por máquina en la primera memoria que contengan comandos que eviten la ejecución del algoritmo J-PAKE después de que se almacene la clave de cifrado de Bluetooth en la primera memoria. Estas primeras instrucciones de máquina o incluso la implementación del propio algoritmo J-PAKE se podrían modificar de modo que se elimine o sobrescriba todo o una parte del algoritmo J-PAKE en la primera memoria. Esto haría imposible inducir al aparato eléctrico médico a pasar por el procedimiento de emparejamiento de Bluetooth por segunda vez, incluso si el dispositivo se pirateara.

En otro modo de realización, el algoritmo de concordancia de clave autenticada por contraseña es un algoritmo EKE.

En otro modo de realización, el algoritmo de concordancia de clave autenticada por contraseña es un algoritmo PPK.

En otro modo de realización, el algoritmo de concordancia de clave autenticada por contraseña es un algoritmo SPEKE.

En otro modo de realización, el algoritmo de concordancia de clave autenticada por contraseña es un algoritmo Dragonfly.

En otro modo de realización, el algoritmo de concordancia de clave autenticada por contraseña cumple con la norma IEEE 802.11-2012.

En otro modo de realización, el sistema electrónico tiene una superficie exterior. El aparato eléctrico médico también se puede denominar en el presente documento sistema electrónico. La superficie exterior comprende una etiqueta con datos de contraseña. Los datos de contraseña son descriptivos de la contraseña de un solo uso. En algunos casos, los datos de contraseña pueden ser idénticos a la contraseña de un solo uso. En otros ejemplos, los datos de contraseña pueden comprender datos que se pueden transformar en la contraseña de un solo uso. Por ejemplo, cuando los datos de la contraseña se pasan a través de una función resumen, se pueden convertir en la contraseña apropiada. Los datos de contraseña también pueden ser un código legible por máquina que se puede transformar en la contraseña. En otro ejemplo, los datos de contraseña comprenden también el número de serie del aparato eléctrico médico. En algunos casos, la contraseña de un solo uso y el número de serie están en los datos de contraseña. En algunos casos, la contraseña de un solo uso es o comprende el número de serie del aparato eléctrico médico.

En otro modo de realización, la interfaz de entrada de datos comprende un teclado. El procedimiento comprende además la etapa de introducir la contraseña de un solo uso y/o los datos de contraseña usando el teclado. Por ejemplo, si la unidad de control tiene una pantalla táctil, el procedimiento puede comprender visualizar el teclado en la pantalla táctil de modo que se pueda completar la etapa de introducir la contraseña de un solo uso usando la pantalla táctil.

En otro modo de realización, el instrumento médico comprende además material impreso que comprende la contraseña de un solo uso. El material impreso puede ser, por ejemplo, una hoja de papel que se incluye con el aparato eléctrico médico que contiene cosas tales como la contraseña de un solo uso y/o el número de serie del aparato eléctrico médico.

En otro modo de realización, la etiqueta es legible por máquina. La interfaz de entrada de datos es un lector óptico de etiquetas configurado para leer los datos de contraseña. El lector óptico de etiquetas puede adoptar diferentes formas dependiendo del tipo de etiqueta diferente. En algunos casos, el lector óptico de etiquetas es una cámara. En otros casos, se pueden usar cosas tales como un escáner láser. La etapa de introducir la contraseña de un solo uso en la interfaz de entrada de datos comprende leer los datos de contraseña con el lector óptico de etiquetas. La etapa de introducir la contraseña de un solo uso en la interfaz de entrada de datos comprende además transformar los datos de contraseña en la contraseña de un solo uso. Por ejemplo, si la etiqueta contiene la contraseña de un

solo uso y el número de serie, esta etapa puede incluir extraer la contraseña de un solo uso de la información o datos del lector óptico.

En otro modo de realización, los datos de contraseña están codificados como un código de barras y el lector óptico de etiquetas es un lector de código de barras.

En otro modo de realización, los datos de contraseña están codificados como un código EAN y el lector óptico de etiquetas es un lector de códigos EAN.

En otro modo de realización, los datos de contraseña están codificados como un código óptico bidimensional y el lector óptico de etiquetas es un lector de códigos ópticos bidimensionales.

En otro modo de realización, los datos de contraseña están codificados como un código QR y el lector óptico de etiquetas es un lector de códigos QR.

En otro modo de realización, los datos de contraseña están codificados como un código de matriz de datos y el lector óptico de etiquetas es un lector de códigos de matriz de datos.

En los ejemplos anteriores, por ejemplo, el lector de códigos de barras, el lector de códigos EAN, el lector de códigos ópticos bidimensionales y el lector de códigos QR se pueden implementar en algunos ejemplos como una cámara con un programa informático apropiado para analizar imágenes tomadas por la cámara.

En otro modo de realización, el lector óptico de etiquetas es una cámara digital.

En otro modo de realización, la parte electrónica comprende un indicador óptico. El indicador óptico en un ejemplo puede ser una luz o un diodo emisor de luz que puede destellar. La interfaz de entrada de datos comprende un detector óptico. El detector óptico puede ser, por ejemplo, una cámara digital o puede ser otro detector para detectar señales del indicador óptico. En algunos ejemplos, el indicador óptico y el detector óptico podrían estar operativos para funcionar en el intervalo infrarrojo o ultravioleta. La etapa de introducir la contraseña de un solo uso en la interfaz de entrada de datos comprende transmitir la contraseña de un solo uso usando el indicador óptico. La etapa de introducir la contraseña de un solo uso en la interfaz de entrada de datos comprende además recibir la contraseña de un solo uso usando el detector óptico.

En otro modo de realización, la parte electrónica comprende un generador de señales de audio. El generador de señales de audio puede ser, por ejemplo, un altavoz, un transductor piezoeléctrico u otro transductor usado para generar sonidos de audio. La interfaz de entrada de datos comprende un detector de señales de audio. El detector de señales de audio, por ejemplo, puede ser un micrófono. La etapa de introducir la contraseña de un solo uso en la interfaz de entrada de datos comprende transmitir la contraseña de un solo uso usando el generador de señales de audio. La etapa de introducir la contraseña de un solo uso en la interfaz de entrada de datos comprende además recibir la contraseña de un solo uso usando el generador de señales de audio.

Por ejemplo, el generador de señales de audio podría usar uno o múltiples tonos para transmitir los datos. Por ejemplo, una única frecuencia de alrededor de 3 kHz puede ser útil. En este caso se podría realizar la modificación de amplitud de la señal de audio. Si se usan una segunda o más frecuencias, se podría usar una de las frecuencias como señal de reloj. Esto puede posibilitar una transmisión más rápida de los datos.

En otro modo de realización, el aparato eléctrico médico tiene un interruptor para que el aparato eléctrico médico comience a transmitir la contraseña de un solo uso.

En otro modo de realización, la parte electrónica comprende un primer módulo de RFID. La interfaz de entrada de datos es un segundo módulo de RFID. La etapa de introducir la contraseña de un solo uso en la interfaz de entrada de datos comprende intercambiar la contraseña de un solo uso usando el primer módulo de RFID y el segundo módulo de RFID. El uso del módulo de RFID puede ser útil porque RFID tiene un alcance más corto que Bluetooth. Además, el uso de dos protocolos de comunicación diferentes puede reducir las posibilidades de que se robe la contraseña de un solo uso y se eluda el procedimiento.

En otro modo de realización, el primer módulo de RFID está controlado por el primer procesador.

En otro modo de realización, el primer módulo de RFID es una etiqueta RFID. Por ejemplo, la etiqueta RFID se podría montar internamente o en una superficie externa del aparato eléctrico médico. En algunos casos, la etiqueta RFID también puede combinar una etiqueta legible por máquina. La etiqueta RFID comprende una memoria de etiqueta RFID y la memoria de etiqueta RFID contiene la contraseña de un solo uso. En este caso, tanto la primera memoria como la memoria de etiqueta RFID contienen la contraseña de un solo uso. El uso de una etiqueta RFID fijada al aparato eléctrico médico puede ser útil porque el usuario podría, por ejemplo, retirar y/o destruir la etiqueta RFID después de su uso.

En otro modo de realización, la parte electrónica comprende un primer módulo de NFC. La interfaz de entrada de datos es un segundo módulo de NFC. La etapa de introducir los datos de contraseña en la interfaz de entrada de datos comprende intercambiar los datos de contraseña usando el primer módulo de NFC y el segundo módulo de NFC.

En otro modo de realización, el aparato eléctrico médico comprende una bomba de insulina.

En otro modo de realización, el aparato eléctrico médico comprende una bomba de glucagón.

En otro modo de realización, el aparato eléctrico médico comprende un sistema de supervisión continua de glucosa.

En otro modo de realización, la unidad de control es un dispositivo de teléfono móvil o un ordenador de tableta.

En otro modo de realización, la contraseña de un solo uso tiene una entropía menor que la clave de cifrado de Bluetooth.

En otro modo de realización, la etapa de introducir la contraseña de un solo uso en la interfaz de entrada de datos comprende: introducir los datos de contraseña en la interfaz de entrada de datos, en la que los datos de contraseña son descriptivos de la contraseña de un solo uso; y transformar los datos de contraseña en la contraseña de un solo uso.

En otro aspecto, la invención proporciona un instrumento médico. El instrumento médico comprende un aparato eléctrico médico y una unidad de control. El aparato eléctrico médico está alimentado por pila por una primera pila. La unidad de control está alimentada por pila por una segunda pila. El aparato eléctrico médico comprende una parte electrónica y una parte subcutánea. La parte electrónica comprende un primer procesador y una primera memoria. La primera memoria contiene una contraseña de un solo uso. La primera memoria contiene además una implementación de un algoritmo de concordancia de clave autenticada por contraseña. La primera memoria contiene además las primeras instrucciones ejecutables por máquina. La unidad de control comprende un segundo procesador y una segunda memoria. La unidad de control comprende una interfaz de entrada de datos.

La segunda memoria contiene la implementación del algoritmo de concordancia de clave autenticada por contraseña. La segunda memoria contiene además segundas instrucciones ejecutables por máquina. El aparato eléctrico médico comprende un primer módulo de comunicación Bluetooth. La unidad de control comprende además un segundo módulo de comunicación Bluetooth. El primer módulo de comunicación Bluetooth y el segundo módulo de comunicación Bluetooth son operativos para formar un canal de comunicación inalámbrica entre el aparato eléctrico médico y la unidad de control. La ejecución de las segundas instrucciones ejecutables por máquina hace que el segundo procesador reciba la contraseña de un solo uso en la interfaz de entrada de datos.

En algunos ejemplos, la ejecución de las primeras instrucciones ejecutables por máquina puede hacer que el primer procesador transmita la contraseña de un solo uso a la interfaz de entrada de datos. Por ejemplo, si el aparato eléctrico médico transmite la contraseña de un solo uso por medio de ondas sonoras, de luz, imagen u radio. La ejecución de las segundas instrucciones ejecutables por máquina y las primeras instrucciones ejecutables por máquina hace que el primer procesador y el segundo procesador generen una clave de cifrado de Bluetooth por el aparato eléctrico médico y la unidad de control con la contraseña de un solo uso intercambiando datos a través del canal de comunicación inalámbrica ejecutando el algoritmo de concordancia de clave autenticada por contraseña.

La unidad de control inicia la ejecución del algoritmo de concordancia de clave autenticada por contraseña. La ejecución de las primeras instrucciones ejecutables por máquina hace que el primer procesador almacene la clave de cifrado de Bluetooth en la primera memoria. La ejecución de las primeras instrucciones hace además que el primer procesador desactive el algoritmo de concordancia de clave autenticada por contraseña en la primera memoria después de almacenar la clave de cifrado de Bluetooth en la primera memoria. La ejecución de las segundas instrucciones ejecutables por máquina hace que el segundo procesador almacene la clave de cifrado de Bluetooth en la segunda memoria. La ejecución de las segundas instrucciones ejecutables por máquina y las primeras instrucciones ejecutables por máquina hace que el primer procesador y el segundo procesador establezcan un canal de comunicación Bluetooth cifrado usando el primer módulo de comunicación Bluetooth y el segundo módulo de comunicación Bluetooth. El canal de comunicación Bluetooth cifrado se cifra usando la clave de cifrado de Bluetooth.

El documento pertinente de la técnica anterior US 2014/281547 también divulga un procedimiento para hacer funcionar un instrumento médico donde se ingresa una contraseña de un solo uso, se genera una clave de cifrado de Bluetooth y se almacena en la memoria y posteriormente se usa para establecer un canal de comunicación Bluetooth cifrado. Sin embargo, este documento de la técnica anterior no divulga ni sugiere desactivar el algoritmo de concordancia de clave autenticada por contraseña en la memoria del instrumento médico después de que se ha generado y almacenado en dicha memoria la clave de cifrado de Bluetooth.

Breve descripción de los dibujos

En lo que sigue se explican con mayor detalle modos de realización de la invención, solo a modo de ejemplo, haciendo referencia a los dibujos en los que:

la fig. 1 ilustra un ejemplo de un instrumento médico;

la fig. 2 ilustra otro ejemplo de un instrumento médico;

la fig. 3 muestra un diagrama de flujo que ilustra un ejemplo de un procedimiento de funcionamiento de un instrumento médico;

la fig. 4 ilustra otro ejemplo de un instrumento médico;

la fig. 5 ilustra otro ejemplo de un instrumento médico;

la fig. 6 ilustra otro ejemplo de un instrumento médico;

la fig. 7 ilustra otro ejemplo de un instrumento médico;

la fig. 8 ilustra la relación funcional de un algoritmo J-PAKE y un sistema de comunicación Bluetooth; y

la fig. 9 muestra un diagrama de flujo que ilustra un procedimiento que usa el algoritmo J-PAKE para generar claves de seguridad de Bluetooth.

Descripción detallada

Los elementos numerados similarmente en estas figuras son elementos equivalentes o bien realizan la misma función. Los elementos que se han analizado previamente no se analizarán necesariamente en figuras posteriores si la función es equivalente.

La fig. 1 muestra un ejemplo de un instrumento médico 100. El instrumento médico comprende una unidad de control 102 y un aparato eléctrico médico 104. Se muestra que el aparato eléctrico médico 104 está en una base 106 que tiene una capa adhesiva 108 que lo fija a la capa externa 110 de un sujeto 112. La vista del sujeto 112 es en sección transversal. Se muestra que la superficie exterior 110 está en contacto con la dermis o una capa cutánea 114. La dermis está en contacto con el tejido adiposo 116. Se muestra que el aparato eléctrico médico 104 tiene una parte electrónica 118 y una parte subcutánea 120. La parte subcutánea comprende una cánula 124 y un sensor 130 fijado a un cable de sensor 128. En este ejemplo, la parte electrónica 118 contiene una bomba 122 que está conectada a la cánula 124 que se extiende en el tejido adiposo 116. Por ejemplo, la bomba 122 se podría usar para dosificar insulina y/o glucagón. En algunos casos, puede haber más de una bomba de modo que se puedan dosificar tanto insulina como glucagón. Se muestra además que la parte electrónica 118 tiene un controlador de sensor 126 que está conectado al cable de sensor 128 que se extiende en el sujeto 112. El sensor 130 podría ser, por ejemplo, un sensor de glucosa para un sistema de supervisión continua de glucosa.

Se muestra adicionalmente que la parte electrónica 118 comprende un primer procesador 132, un primer módulo de comunicación Bluetooth 134 y una primera pila 136. En la fig. 1 no se muestran todos los componentes de la unidad de control 102 y el aparato eléctrico médico 104.

Se muestra que la unidad de control 102 tiene una pantalla táctil 138. En la pantalla táctil 138 se implementa un panel táctil 140. Por ejemplo, el panel táctil 140 se podría usar para introducir la contraseña de un solo uso. La pantalla táctil 138 también podría tener otros elementos tales como un recuadro o elemento de visualización 142 para mostrar los datos que se escribieron. No todos los componentes de la unidad de control 102 se muestran en esta fig. Se muestra que la unidad de control 102 comprende además un segundo procesador 144 que está alimentado por una segunda pila 148. La unidad de control 102 comprende además un segundo módulo Bluetooth 150 que se usa para formar un canal de comunicación inalámbrica 152 entre la unidad de control 102 y el aparato eléctrico médico 104. La unidad de control 102 a continuación puede enviar y recibir datos por medio del canal de comunicación inalámbrica 152 para controlar y/o supervisar el funcionamiento del aparato eléctrico médico 104.

La fig. 2 muestra otro ejemplo del instrumento médico 200. El instrumento médico 200 tiene una superficie exterior 202 a la que se fija una etiqueta legible por máquina 204. La etiqueta legible por máquina 204 puede codificar datos de contraseña que son descriptivos o se pueden usar para derivar la contraseña de un solo uso. En este ejemplo, se muestra además que la parte electrónica 118 contiene una primera memoria 206 y una interfaz de equipo informático 208. La interfaz de equipo informático 208 posibilita que el procesador 132 controle el funcionamiento y función de los componentes del aparato eléctrico médico. No todos los componentes se muestran en la fig. 2.

Se muestra que la primera memoria 206 tiene una contraseña de un solo uso 210 almacenada dentro de ella. Se muestra que la primera memoria 206 contiene además un algoritmo de concordancia de clave autenticada por contraseña 212. Se muestra además que la primera memoria 206 contiene un módulo de control 214 que proporciona código que posibilita que el procesador 132 controle el funcionamiento y función de todo el aparato médico. Se muestra además que la primera memoria 206 contiene un registro de datos 216. El registro de datos contiene datos que se pueden generar o almacenar a medida que el procesador 132 implementa el módulo de control 214. Por ejemplo, cómo se pueden almacenar en este archivo los datos de sensor 130 de la bomba 122. Se muestra además que la primera memoria 206 contiene una clave de cifrado de Bluetooth 218 que se derivó tras la ejecución del algoritmo de concordancia de clave autenticada por contraseña 212. Se muestra además que la primera memoria 206 contiene instrucciones de la unidad de control 220 que se reciben por medio del canal de comunicación inalámbrica 152.

En este ejemplo particular, se muestra que la unidad de control 102 comprende además una cámara 221 y una segunda memoria 223. Se muestra que la cámara 221 se sitúa de modo que pueda sacar una imagen de la etiqueta legible por máquina 204. Se muestra que la segunda memoria 223 contiene un sistema operativo 222 que proporciona el sistema operativo para la unidad de control 102. Por ejemplo, el sistema operativo 222 puede ser Android, iOS, LINUX u otro sistema operativo. Se muestra además que la segunda memoria 223 contiene una aplicación de control 224 que posibilita que el procesador 144 controle el aparato eléctrico médico 104 por medio del canal de comunicación inalámbrica 152. La cámara 221 se puede usar para sacar una imagen de la etiqueta legible por máquina 204. Se muestra que la segunda memoria 223 contiene en este caso una imagen que se identifica como datos de contraseña 226. Se muestra que la segunda memoria 223 contiene además un módulo de transformación de contraseña 228 que posibilita que el procesador 114 descodifique la imagen o datos de contraseña 226 en la contraseña de un solo uso 210. Se muestra además que la memoria de ordenador 223 contiene una implementación del algoritmo de concordancia de clave autenticada por contraseña 212'. Las instrucciones ejecutables por máquina 212 y 212' posibilitan que la unidad de control 102 y el aparato eléctrico médico 104 generen la clave de cifrado de Bluetooth 218 usando la contraseña de un solo uso 210 como un secreto compartido. Los rasgos característicos de la fig. 1 y la fig. 2 se pueden combinar. En el ejemplo mostrado en la fig. 2, una vez que la cámara 221 ha sacado una imagen de la etiqueta legible por máquina 204, esto puede iniciar la implementación del algoritmo de concordancia de clave autenticada por contraseña.

La fig. 3 muestra un ejemplo de un procedimiento ilustrado en un diagrama de flujo que muestra cómo se puede hacer funcionar un instrumento médico de acuerdo con un ejemplo. En primer lugar, en la etapa 300, se introduce la contraseña de un solo uso 210 en la interfaz de entrada de datos 140. Esta etapa también se puede proporcionar usando la cámara 221 u otros ejemplos que siguen en las figs. posteriores. Seguidamente, en la etapa 302 se genera una clave de cifrado de Bluetooth 218 por el aparato eléctrico médico 104 y la unidad de control 102 intercambiando datos a través del canal de comunicación inalámbrica 152. Esto se hace ejecutando el algoritmo de concordancia de clave autenticada por contraseña 212, 212', la unidad de control 102 inicia la ejecución del algoritmo de concordancia de clave autenticada por contraseña 212, 212'.

Seguidamente, en la etapa 304 se almacena la clave de cifrado de Bluetooth 218 en la primera memoria 206. La siguiente etapa es la etapa 306 donde se desactiva el algoritmo de concordancia de clave autenticada por contraseña 212 después de almacenar la clave de cifrado de Bluetooth 218 en la primera memoria 206. Seguidamente, en la etapa 308 se almacena la clave de cifrado de Bluetooth 218 en la segunda memoria 223. Finalmente, en la etapa 310 se establece un canal de comunicación Bluetooth cifrado 152 usando el primer módulo de comunicación Bluetooth 134 y el segundo módulo de comunicación Bluetooth 150. El canal de comunicación Bluetooth es el canal de comunicación inalámbrica 152 que se ha cifrado usando la clave de cifrado de Bluetooth 218.

La fig. 4 muestra otro ejemplo del aparato médico 400. En este ejemplo, en lugar de haber una etiqueta 204, hay una fuente de luz o luz 402 que se expone a la superficie externa 202 o visible cuando se mira la superficie externa 202. La primera memoria 206 contiene los datos de contraseña 226. En este caso, los datos de contraseña 226 son la contraseña sin tiempo 210 codificada como impulsos para la luz 402. El procesador 132 a continuación controla la luz 402 para que parpadee de acuerdo con los datos de contraseña 226. La cámara 221 a continuación registra estos impulsos y los registra como los datos de contraseña 226. Otros tipos de detectores ópticos 221 podrían sustituir a la cámara 221.

La fig. 5 muestra otro ejemplo de un aparato médico 500. El ejemplo mostrado en la fig. 5 es similar al de la fig. 4 excepto que la luz se ha reemplazado por un transductor 502. La cámara 221 se ha reemplazado por un micrófono 504. El transductor 502 puede transmitir ondas sonoras 506 al micrófono 504. En este ejemplo, los datos de contraseña 226 están codificados como un sonido que se puede transmitir desde el transductor 502 al micrófono 504 por medio de las ondas sonoras 506, donde a continuación se registran de nuevo y se almacenan como un sonido o datos de contraseña 226. El registro de los datos de contraseña 226 por el micrófono 504 puede provocar que el procesador 144 inicie el algoritmo de concordancia de clave autenticada por contraseña 212'.

La fig. 6 muestra otro ejemplo de un aparato médico 600. En este ejemplo, el aparato eléctrico médico 104 comprende un primer módulo de RFID 602 y la unidad de control 102 comprende un segundo módulo de RFID 604.

Estos dos módulos de RFID 602, 604 pueden formar un canal de comunicación de RFID 606 que se usa para intercambiar los datos de contraseña 226 o incluso la contraseña de un solo uso 210 directamente por medio del canal de comunicación de RFID 606.

La fig. 7 muestra otro ejemplo de un aparato médico 700. El ejemplo mostrado en la fig. 7 es similar al de la fig. 6 excepto que en lugar de que el procesador 132 controle el primer módulo de RFID 602, el primer módulo de RFID 602' es una etiqueta RFID. La etiqueta RFID 602' tendrá una memoria separada que almacenará la contraseña de un solo uso o los datos de contraseña 226 por separado de la primera memoria 206. El segundo módulo de RFID 604 funciona como un lector de RFID para la etiqueta RFID 602'.

Los protocolos de comunicación estandarizados como Bluetooth permiten que los dispositivos se comuniquen entre sí. Por motivos de seguridad es necesario poder reconocer dispositivos específicos y, por tanto, posibilitar el control sobre qué dispositivos se permite la conexión a un dispositivo de Bluetooth dado. Lamentablemente, los protocolos de Bluetooth disponibles para el emparejamiento, como el emparejamiento simple seguro en la versión 4.0 de Bluetooth, no protegen eficazmente contra ataques de intermediarios o MITM y, además, requieren que cada dispositivo tenga un componente de entrada tal como una pantalla y/o teclados numéricos. La desventaja de los protocolos disponibles de Bluetooth estándar para el emparejamiento no protegen contra los ataques MITM, especialmente si uno o ambos dispositivos no tenían un componente de entrada como es el caso de una bomba de parche. Una bomba de parche es una bomba de insulina que se fija a la superficie del sujeto.

Algunos ejemplos pueden usar una combinación específica que comprende un protocolo de concordancia de clave autenticado por contraseña, tal como J-PAKE, que tiene una interfaz con un protocolo de baja energía de Bluetooth estandarizado en el que se almacena el número aleatorio de alta seguridad generado. Una solución técnica es que el algoritmo J-PAKE genere un número aleatorio para emparejar ambos dispositivos en base a números aleatorios generados por cada dispositivo y una contraseña, en este caso, una contraseña de un solo uso. La contraseña se puede imprimir, por ejemplo, en el dispositivo médico, por ejemplo, como un código de barras, un código 2D o código de matriz de puntos y leerse, por ejemplo, con una cámara integrada en el controlador remoto. El número aleatorio altamente seguro se integra a continuación en el apilamiento BLE y permite el emparejamiento seguro entre los dispositivos médicos. Además de J-PAKE, se pueden usar otros protocolos estándar. El algoritmo J-PAKE se puede implementar, por ejemplo, usando curvas elípticas.

La fig. 8 ilustra cómo se puede combinar un algoritmo J-PAKE estándar 212, 212' con una implementación de Bluetooth estándar 800. El algoritmo J-PAKE 212, 212' proporciona un número aleatorio o secreto compartido 210 al gestor de seguridad de Bluetooth 802. A continuación, esto se usa por el módulo de comunicación Bluetooth 804 para establecer una conexión inicial 152 que posibilita el intercambio de números del algoritmo J-PAKE 212, 212' para intercambiar números aleatorios con el aparato eléctrico médico 104.

La fig. 9 muestra un diagrama de flujo que ilustra un ejemplo de integración del algoritmo J-PAKE 212, 212' con Bluetooth 901. En primer lugar, en la etapa 900, el aparato eléctrico médico almacena un número aleatorio 900. Seguidamente, en la etapa 902, la unidad de control comienza el cifrado enviando un mensaje al aparato eléctrico médico 104. En la etapa 904, la unidad de control 102 genera un número aleatorio. Seguidamente, en la etapa 906, la unidad de control 102 envía un número aleatorio al aparato eléctrico médico 104. En la etapa 908, el aparato eléctrico médico envía sus números aleatorios 908 a la unidad de control 102. Después de esto, el aparato eléctrico médico 104 calcula una clave de cifrado de Bluetooth 910. La unidad de control 912 también calcula a continuación la misma clave de cifrado de Bluetooth. A continuación, el algoritmo de concordancia de clave autenticada por contraseña 212, 212' pasa la clave de cifrado de Bluetooth al algoritmo Bluetooth estándar. En la etapa 914, el aparato eléctrico médico envía la clave de cifrado de Bluetooth al gestor de seguridad de Bluetooth. También en la etapa 914, la unidad de control 102 envía su valor calculado para la clave de cifrado de Bluetooth a su gestor de seguridad de Bluetooth. Seguidamente, en la etapa 916, la unidad de control 102 inicia el cifrado de Bluetooth. Seguidamente, en la etapa 918, el aparato eléctrico médico 104 envía un parámetro para el cifrado. Y finalmente, en la etapa 920, la unidad de control 102 envía un mensaje de cifrado de confirmación al aparato eléctrico médico 104. En este punto, se ha establecido un canal de comunicación Bluetooth cifrado.

Lista de números de referencia

100	instrumento médico
102	unidad de control
104	aparato eléctrico médico
106	base
108	adhesivo
110	superficie exterior

112	sujeto
114	dermis
116	tejido adiposo
118	parte electrónica
120	parte subcutánea
122	bomba
124	cánula
126	controlador de sensor
128	cable de sensor
130	sensor
132	procesador
134	primer módulo de comunicación Bluetooth
136	primera pila
138	pantalla táctil
140	teclado
142	elemento de visualización
144	segundo procesador
148	segunda pila
150	segundo módulo de comunicación Bluetooth
152	canal de comunicación inalámbrica
200	instrumento médico
202	superficie exterior
204	etiqueta legible por máquina
206	primera memoria
208	interfaz de equipo informático
210	contraseña de un solo uso
212	algoritmo de concordancia de clave autenticada por contraseña
212'	algoritmo de concordancia de clave autenticada por contraseña
214	módulo de control
216	registro de datos
218	clave de cifrado de Bluetooth
220	instrucciones del controlador
221	cámara

222 sistema operativo

223 segunda memoria

224 aplicación de control

226 datos de contraseña

228 módulo de transformación de contraseña

300 introducir la contraseña de un solo uso en la interfaz de entrada de datos

302 generar una clave de cifrado de Bluetooth por el aparato eléctrico médico y la unidad de control con la contraseña de un solo uso intercambiando datos a través del canal de comunicación inalámbrica ejecutando el algoritmo de concordancia de clave autenticada por contraseña

304 almacenar la clave de cifrado de Bluetooth en la primera memoria;

306 desactivar el algoritmo de concordancia de clave autenticada por contraseña en la primera memoria después de almacenar la clave de cifrado de Bluetooth en la primera memoria;

308 almacenar la clave de cifrado de Bluetooth en la segunda memoria

310 establecer un canal de comunicación Bluetooth cifrado usando el primer módulo de comunicación Bluetooth y el segundo módulo de comunicación Bluetooth

400 aparato médico

402 luz

500 aparato médico

502 transductor

504 micrófono

506 ondas sonoras

600 aparato médico

602 primer módulo de RFID

602' etiqueta RFID

604 segundo módulo de RFID (lector de RFID)

606 canal de comunicación de RFID

700 aparato médico

800 algoritmo Bluetooth

802 gestor de seguridad de Bluetooth

804 comunicación Bluetooth

806 antena

900 Almacenar números aleatorios

901 algoritmo Bluetooth

902 Comenzar cifrado

904 Generar número aleatorio

906 Enviar números aleatorios

908 Enviar números aleatorios

910 Calcular número aleatorio para clave

912 Calcular número aleatorio para clave

914 Enviar clave al gestor de seguridad de BLE

915 Enviar clave al gestor de seguridad de BLE

916 Comenzar cifrado de BLE

918 Enviar parámetro para el cifrado

920 Confirmar cifrado

REIVINDICACIONES

1. Un procedimiento de funcionamiento de un instrumento médico (100, 200, 400, 500, 600, 700), en el que el instrumento médico comprende un aparato eléctrico médico (104) y una unidad de control (102), en el que el aparato eléctrico médico está alimentado por pila por una primera pila (136), en el que la unidad de control está alimentada por pila por una segunda pila (148), en el que el aparato eléctrico médico comprende una parte electrónica (118) y una parte subcutánea (120), en el que la parte electrónica comprende un primer procesador (132) y una primera memoria (206), en el que la primera memoria contiene una contraseña de un solo uso (210), en el que la primera memoria comprende además una implementación de un algoritmo de concordancia de clave autenticada por contraseña (212, 800, 901);

en el que la unidad de control comprende un segundo procesador (144) y una segunda memoria (223), en el que la unidad de control comprende una interfaz de entrada de datos (140, 221, 504, 604), en el que la segunda memoria contiene la implementación del algoritmo de concordancia de clave autenticada por contraseña (212'),

en el que el aparato eléctrico médico comprende un primer módulo de comunicación Bluetooth (134),

en el que la unidad de control comprende además un segundo módulo de comunicación Bluetooth (150), en el que el primer módulo de comunicación Bluetooth y el segundo módulo de comunicación Bluetooth son operativos para formar un canal de comunicación inalámbrica (152) entre el aparato eléctrico médico y la unidad de control, en el que el procedimiento comprende las etapas de:

- introducir (300) la contraseña de un solo uso en la interfaz de entrada de datos;

- generar (302) una clave de cifrado de Bluetooth (218) por el aparato eléctrico médico y la unidad de control con la contraseña de un solo uso intercambiando datos a través del canal de comunicación inalámbrica ejecutando el algoritmo de concordancia de clave autenticada por contraseña, en el que la unidad de control inicia la ejecución del algoritmo de concordancia de clave autenticada por contraseña;

- almacenar (304) la clave de cifrado de Bluetooth en la primera memoria;

- desactivar (306) el algoritmo de concordancia de clave autenticada por contraseña en la primera memoria después de almacenar la clave de cifrado de Bluetooth en la primera memoria;

- almacenar (308) la clave de cifrado de Bluetooth en la segunda memoria; y

- establecer (310) un canal de comunicación Bluetooth cifrado usando el primer módulo de comunicación Bluetooth y el segundo módulo de comunicación Bluetooth, en el que el canal de comunicación Bluetooth cifrado es el canal de comunicación inalámbrica cifrado usando la clave de cifrado de Bluetooth.

2. El procedimiento de la reivindicación 1, en el que la parte subcutánea comprende un sensor de glucosa (130), en el que el aparato eléctrico médico comprende un sistema de supervisión continua de glucosa (126, 130), en el que el procedimiento comprende la etapa de registrar una medición de glucosa usando el sistema de supervisión continua de glucosa, en el que el procedimiento comprende además la etapa de transferir la medición de glucosa a la unidad de control usando el canal de comunicación Bluetooth cifrado.

3. El procedimiento de la reivindicación 1 o 2, en el que la parte subcutánea comprende al menos una cánula (124), en el que el aparato eléctrico médico comprende un sistema de bombeo (122), en el que el sistema de bombeo comprende una cualquiera de las siguientes: una bomba de insulina para bombear insulina a través de la al menos una cánula, una bomba de glucagón para bombear glucagón a través de la al menos una cánula y combinaciones de las mismas; y en el que el procedimiento comprende además la etapa de controlar el sistema de bombeo por medio del canal de comunicación Bluetooth cifrado por la unidad de control.

4. El procedimiento de la reivindicación 1, 2 o 3, en el que el algoritmo de concordancia de clave autenticada por contraseña es uno cualquiera de los siguientes: algoritmo J-Pake (800, 901), EKE, PAK, PPK, SPEKE, Dragonfly y la norma IEEE 802.11-2012

5. El procedimiento de la reivindicación 1, 2 o 3, en el que el algoritmo de concordancia de clave autenticada por contraseña es un algoritmo J-Pake (800, 901), en el que la desactivación del algoritmo J-PAKE en la primera memoria se realiza modificando el algoritmo J-PAKE en el primer procesador de modo que no se ejecute por el primer procesador una vez que se ha almacenado en la primera memoria la clave de cifrado de Bluetooth.

6. El procedimiento de una cualquiera de las reivindicaciones precedentes, en el que el aparato eléctrico médico tiene una superficie exterior (202), en el que la superficie exterior comprende una etiqueta (204) con datos de contraseña (226), en el que los datos de contraseña son descriptivos de la contraseña de un solo uso.

7. El procedimiento de la reivindicación 6, en el que la interfaz de entrada de datos comprende un teclado (140), en el que el procedimiento comprende además la etapa de introducir la contraseña de un solo uso y/o los datos de contraseña usando el teclado.

8. El procedimiento de la reivindicación 7, en el que el instrumento médico comprende además material impreso que comprende la contraseña de un solo uso.

9. El procedimiento de la reivindicación 6, 7 u 8, en el que la etiqueta es legible por máquina, en el que la interfaz de entrada de datos es un lector óptico de etiquetas (221) configurado para leer los datos de contraseña, en el que la etapa de introducir la contraseña de un solo uso en la interfaz de entrada de datos comprende leer los datos de contraseña con el lector óptico de etiquetas, en el que la etapa de introducir la contraseña de un solo uso en la interfaz de entrada de datos comprende además transformar los datos de contraseña en la contraseña de un solo uso.

10. El procedimiento de la reivindicación 9, en el que uno cualquiera de los siguientes: los datos de contraseña están codificados como un código de barras y el lector óptico de etiquetas es un lector de códigos de barras, los datos de contraseña están codificados como un código EAN y el lector óptico de etiquetas es un lector de códigos EAN, los datos de contraseña están codificados como un código óptico bidimensional y el lector óptico de etiquetas es un lector de códigos ópticos bidimensionales, los datos de contraseña están codificados como un código QR y el lector óptico de etiquetas es un lector de códigos QR, los datos de contraseña están codificados como un código de matriz de datos y el lector óptico de etiquetas es un lector de códigos de matriz de datos, el lector óptico de etiquetas es una cámara digital y combinaciones de los mismos.

11. El procedimiento de una cualquiera de las reivindicaciones precedentes, en el que la parte electrónica comprende un indicador óptico (402), en el que la interfaz de entrada de datos comprende un detector óptico (221), en el que la etapa de introducir la contraseña de un solo uso en la interfaz de entrada de datos comprende transmitir la contraseña de un solo uso usando el indicador óptico, en el que la etapa de introducir la contraseña de un solo uso en la interfaz de entrada de datos comprende además recibir la contraseña de un solo uso usando el detector óptico.

12. El procedimiento de una cualquiera de las reivindicaciones precedentes, en el que la parte electrónica comprende un generador de señales de audio (502), en el que la interfaz de entrada de datos comprende un detector de señales de audio (504), en el que la etapa de introducir la contraseña de un solo uso en la interfaz de entrada de datos comprende transmitir la contraseña de un solo uso usando el generador de señales de audio, en el que la etapa de introducir la contraseña de un solo uso en la interfaz de entrada de datos comprende además recibir la contraseña de un solo uso usando el generador de señales de audio.

13. El procedimiento de una cualquiera de las reivindicaciones de 1 a 4, en el que la parte electrónica comprende un primer módulo de RFID (602, 602'), en el que la interfaz de entrada de datos es un segundo módulo de RFID (604), en el que la etapa de introducir la contraseña de un solo uso en la interfaz de entrada de datos comprende intercambiar la contraseña de un solo uso usando el primer módulo de RFID y el segundo módulo de RFID.

14. El procedimiento de la reivindicación 13, en el que el primer módulo de RFID es una etiqueta RFID (602'), en el que la etiqueta RFID comprende una memoria de etiquetas RFID, en el que la memoria de etiquetas RFID contiene la contraseña de un solo uso.

15. El procedimiento de una cualquiera de las reivindicaciones de 1 a 4, en el que la parte electrónica comprende un primer módulo de NFC, en el que la interfaz de entrada de datos es un segundo módulo de NFC, en el que la etapa de introducir los datos de contraseña en la interfaz de entrada de datos comprende intercambiar los datos de contraseña usando el primer módulo de NFC y el segundo módulo de NFC.

16. El procedimiento de una cualquiera de las reivindicaciones precedentes, en el que la contraseña de un solo uso tiene menor entropía que la clave de cifrado de Bluetooth.

17. El procedimiento de una cualquiera de las reivindicaciones precedentes, en el que la etapa de introducir la contraseña de un solo uso en la interfaz de entrada de datos comprende:

- introducir datos de contraseña en la interfaz de entrada de datos, en el que los datos de contraseña son descriptivos de la contraseña de un solo uso; y

- transformar los datos de contraseña en la contraseña de un solo uso.

18. El procedimiento de una cualquiera de las reivindicaciones precedentes, en el que se proporciona la contraseña de un solo uso a la interfaz de entrada de datos por el aparato eléctrico médico.

19. El procedimiento de una cualquiera de las reivindicaciones precedentes, en el que el aparato eléctrico médico

comprende un número de serie, en el que la contraseña de un solo uso comprende al menos parcialmente el número de serie.

20. Un instrumento médico (100, 200, 400, 500, 600, 700), en el que el instrumento médico comprende un aparato eléctrico médico (104) y una unidad de control (102), en el que el aparato eléctrico médico está alimentado por pila por una primera pila (136), en el que la unidad de control está alimentada por pila por una segunda pila (148), en el que el aparato eléctrico médico comprende una parte electrónica (118) y una parte subcutánea (120), en el que la parte electrónica comprende un primer procesador (132) y una primera memoria (206), en el que la primera memoria contiene una contraseña de un solo uso (210), en el que la primera memoria contiene además una implementación de un algoritmo de concordancia de clave autenticada por contraseña (212, 800, 901), en el que la primera memoria contiene además primeras instrucciones ejecutables por máquina,

en el que la unidad de control comprende un segundo procesador (144) y una segunda memoria (223), en el que la unidad de control comprende una interfaz de entrada de datos (140, 221, 504, 604), en el que la segunda memoria contiene la implementación del algoritmo de concordancia de clave autenticada por contraseña (212'), en el que la segunda memoria contiene además segundas instrucciones ejecutables por máquina,

en el que el aparato eléctrico médico comprende un primer módulo de comunicación Bluetooth (134), en el que la unidad de control comprende además un segundo módulo de comunicación Bluetooth (150), en el que el primer módulo de comunicación Bluetooth y el segundo módulo de comunicación Bluetooth son operativos para formar un canal de comunicación inalámbrica (152) entre el aparato eléctrico médico y la unidad de control, en el que la ejecución de las segundas instrucciones ejecutables por máquina hace que el segundo procesador reciba (300) la contraseña de un solo uso en la interfaz de entrada de datos,

en el que la ejecución de las segundas instrucciones ejecutables por máquina y las primeras instrucciones ejecutables por máquina hace que el primer procesador y el segundo procesador generen (302) una clave de cifrado de Bluetooth (218) por el aparato eléctrico médico y la unidad de control con la contraseña de un solo uso intercambiando datos a través del canal de comunicación inalámbrica ejecutando el algoritmo de concordancia de clave autenticada por contraseña, en el que la unidad de control inicia la ejecución del algoritmo de concordancia de clave autenticada por contraseña,

en el que la ejecución de las primeras instrucciones ejecutables por máquina hace que el primer procesador almacene (304) la clave de cifrado de Bluetooth en la primera memoria;

en el que la ejecución de las primeras instrucciones hace además que el primer procesador desactive (306) el algoritmo de concordancia de clave autenticada por contraseña en la primera memoria después de almacenar la clave de cifrado de Bluetooth en la primera memoria,

en el que la ejecución de las segundas instrucciones ejecutables por máquina hace que el segundo procesador almacene (308) la clave de cifrado de Bluetooth en la segunda memoria,

en el que la ejecución de las segundas instrucciones ejecutables por máquina y las primeras instrucciones ejecutables por máquina hace que el primer procesador y el segundo procesador establezcan (310) un canal de comunicación Bluetooth cifrado usando el primer módulo de comunicación Bluetooth y el segundo módulo de comunicación Bluetooth, en el que el canal de comunicación Bluetooth cifrado es el canal de comunicación inalámbrica cifrado usando la clave de cifrado de Bluetooth.

21. El instrumento médico de la reivindicación 20, en el que el primer procesador desactiva el algoritmo de concordancia de clave autenticada por contraseña en la primera memoria eliminando o sobrescribiendo al menos una parte del algoritmo de concordancia de clave autenticada por contraseña en la primera memoria.

Fig. 1

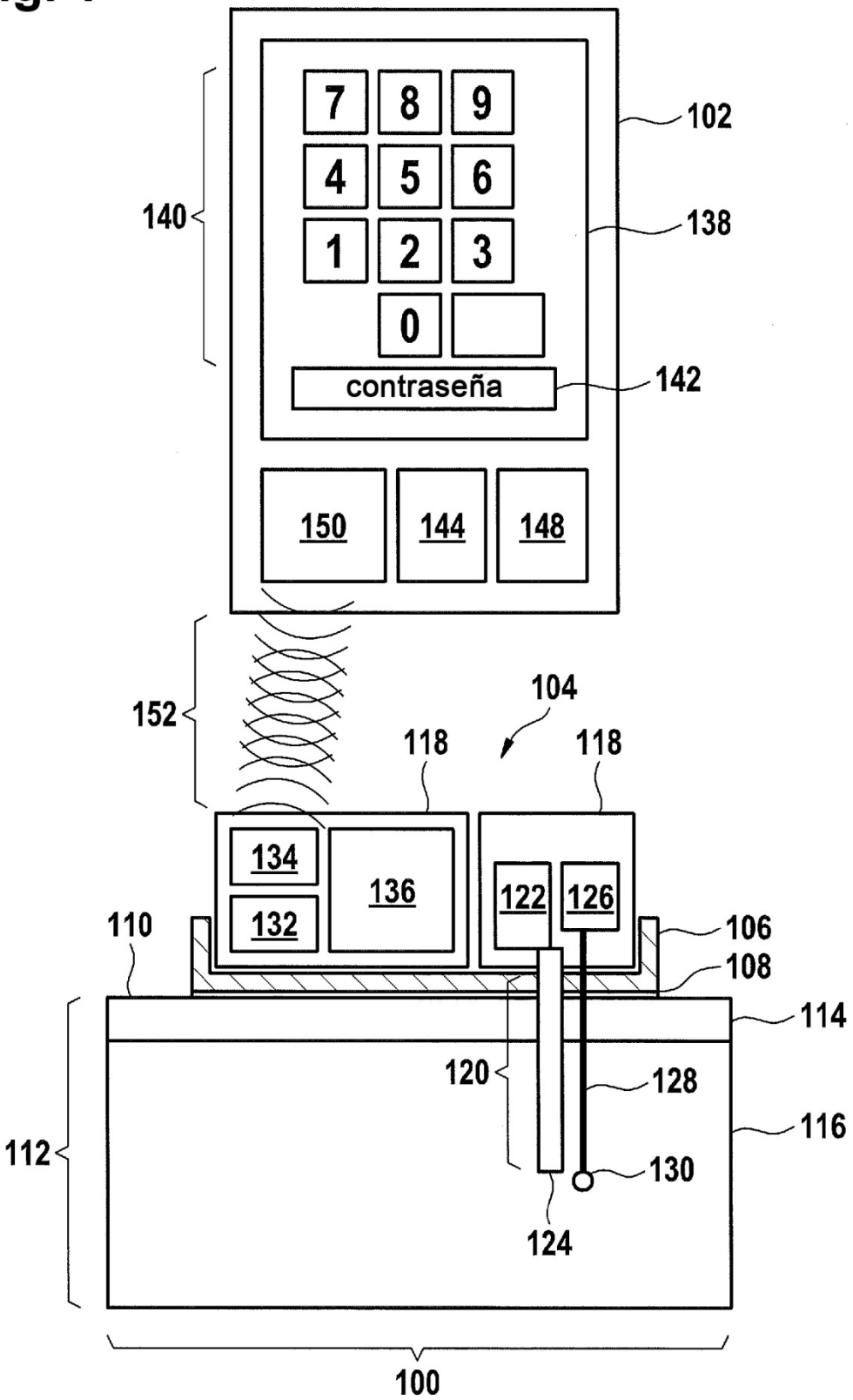

7
8
9
4
5
6
1
2
3
0
contraseña
102
138
140
142
150
144
148
152
104
118
118
134
136
132
122
126
110
106
108
114
120
128
116
112
130
124
100

Fig. 2

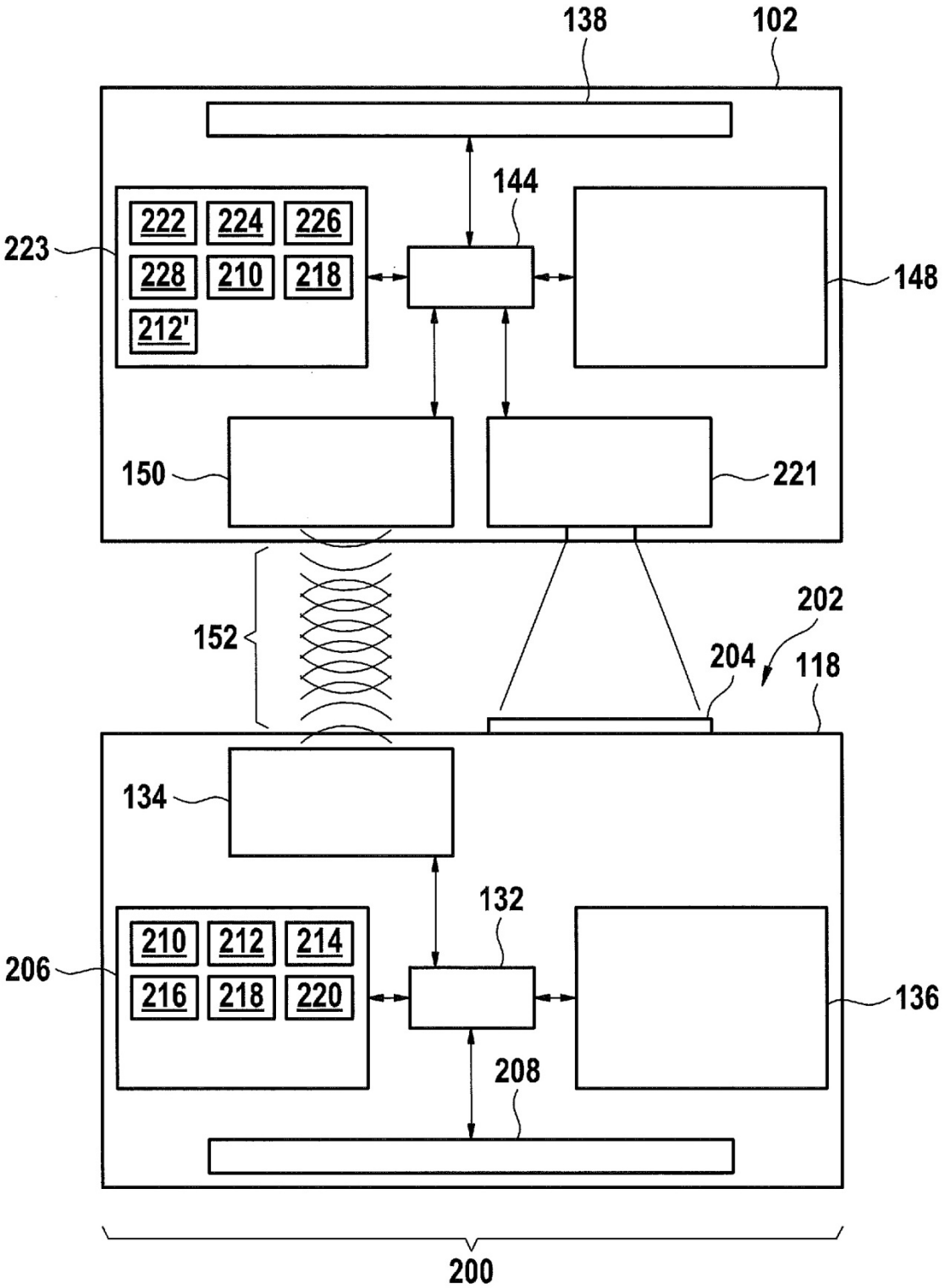

138
102
144
222
224
226
223
228
210
218
212'
148
150
221
152
202
204
118
134
132
210
212
214
206
216
218
220
136
208
200

Fig. 3

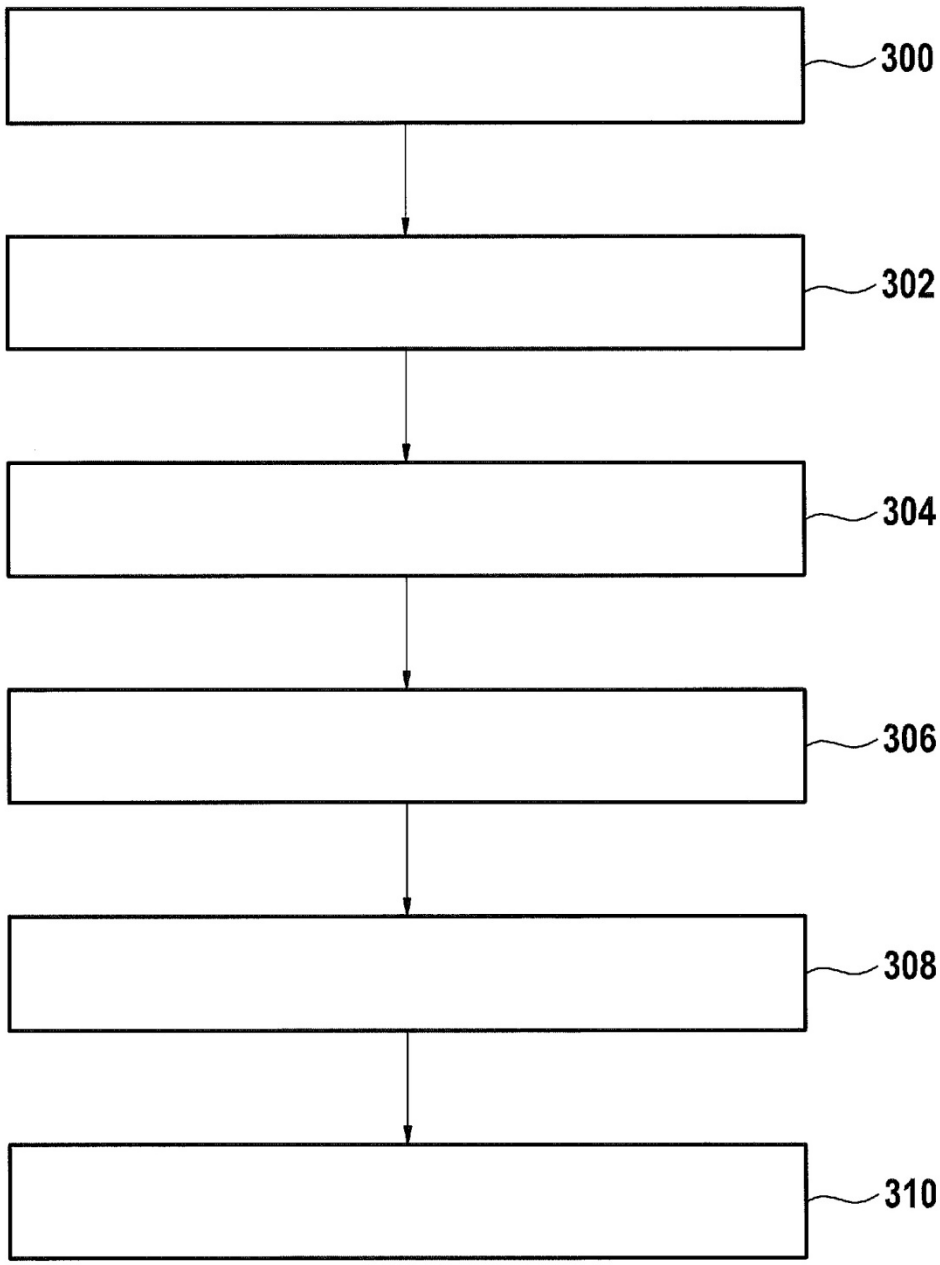


Fig. 4

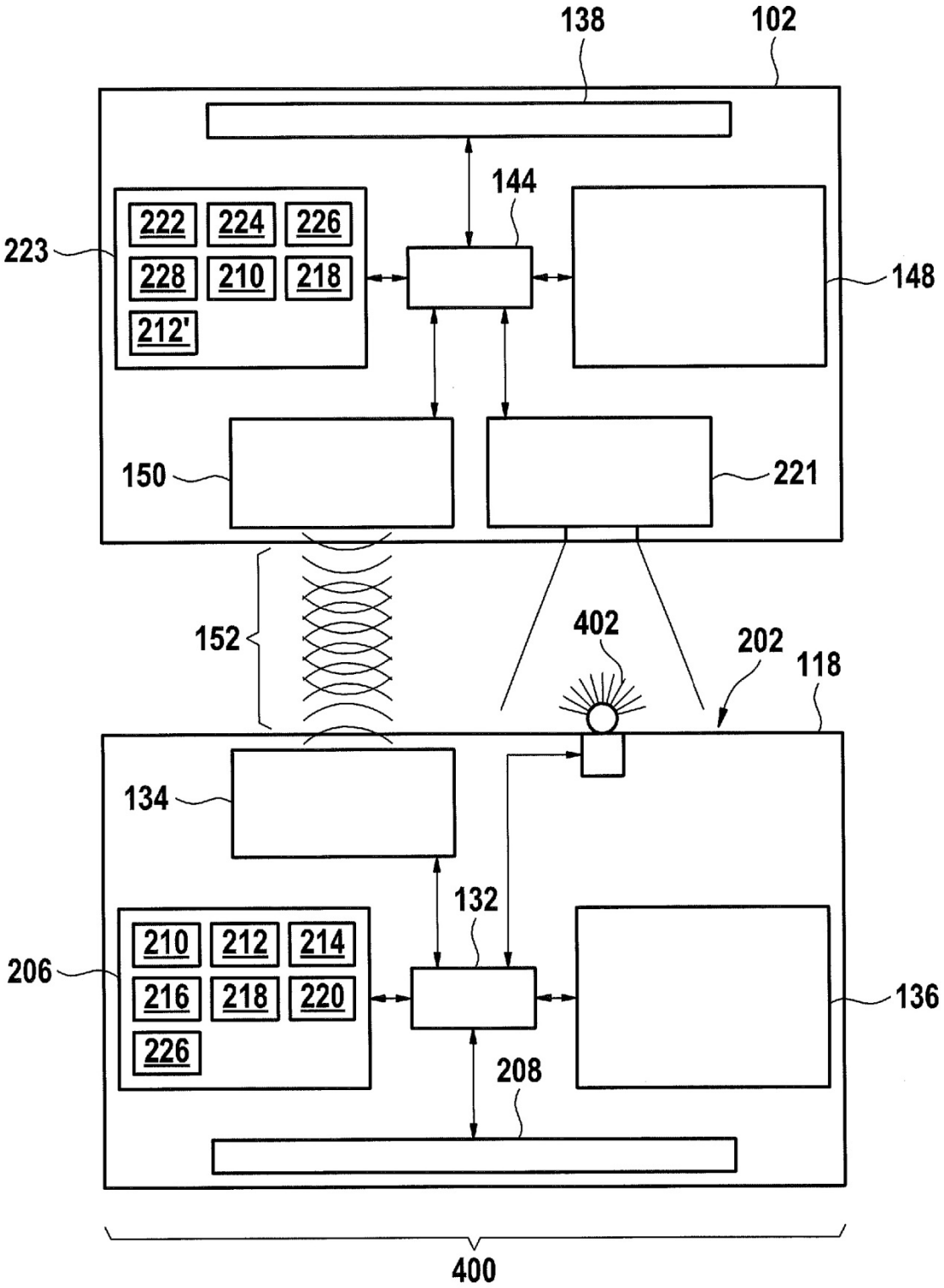

138
102
144
222
224
226
223
228
210
218
212'
148
150
221
152
402
202
118
134
132
210
212
214
206
216
218
220
226
136
208
400

Fig. 5

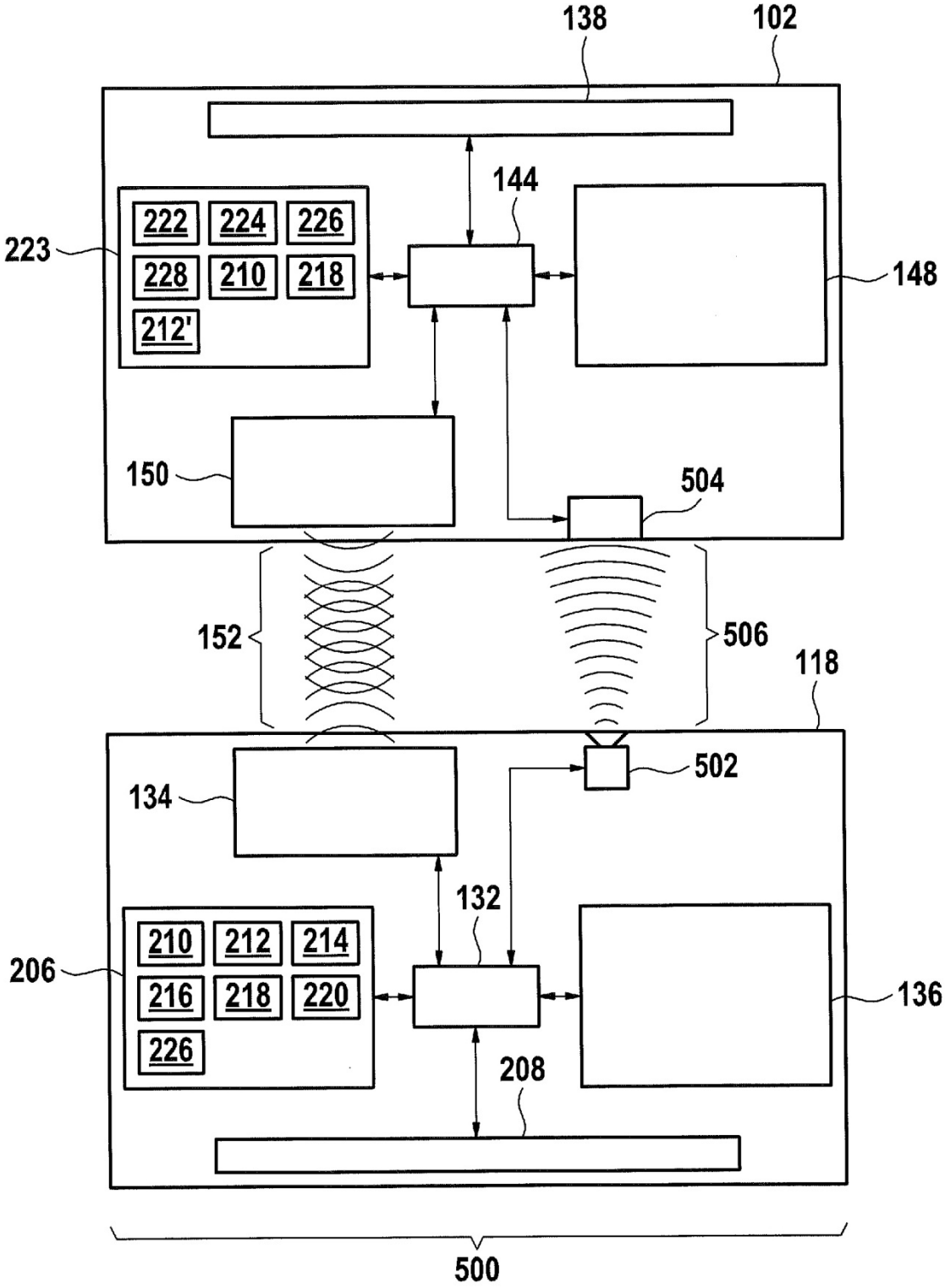

138
102
144
222
224
226
223
228
210
218
212'
148
150
504
152
506
118
502
134
132
210
212
214
206
216
218
220
226
136
208
500

Fig. 6

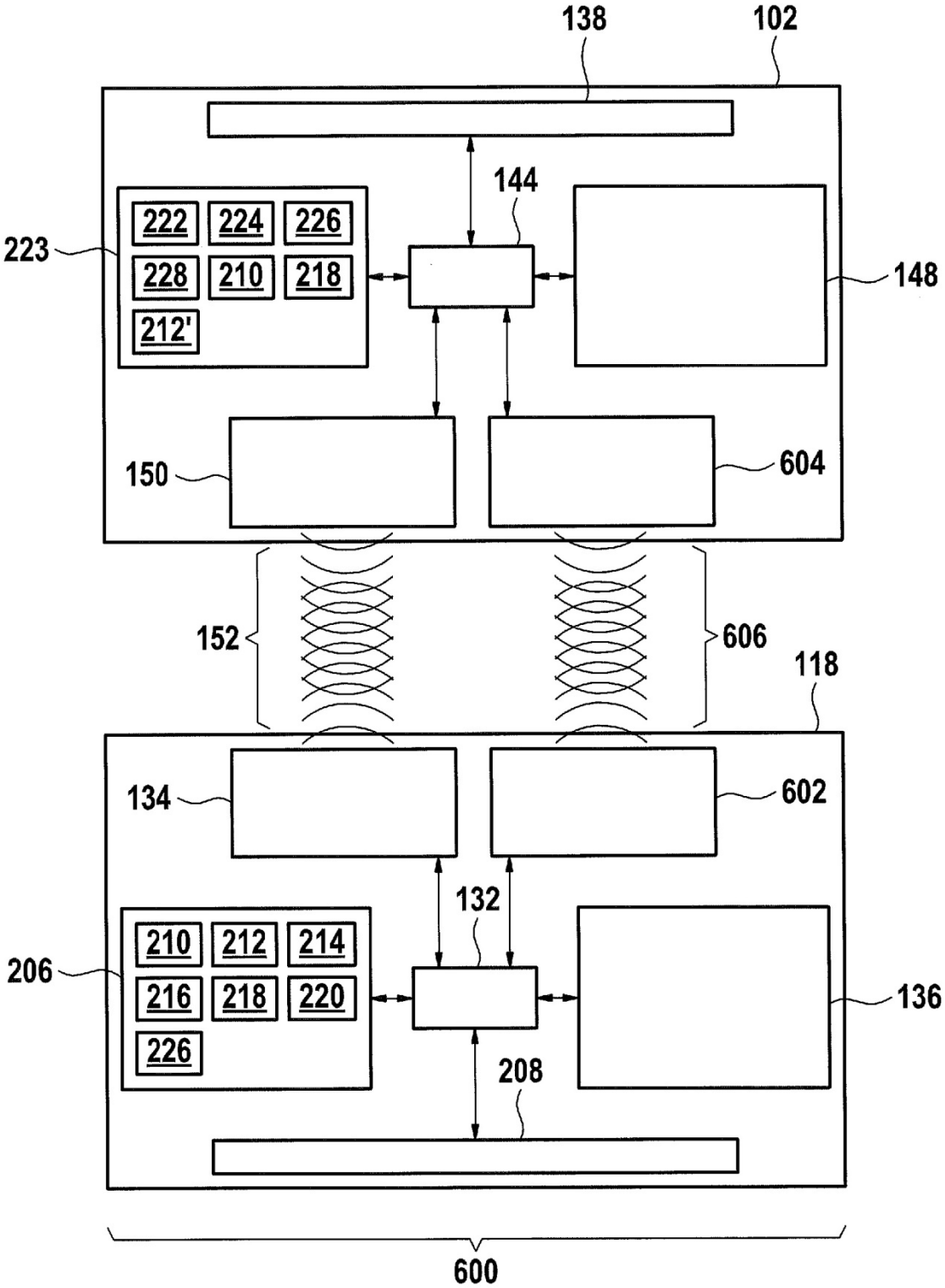

138
102
144
222
224
226
223
228
210
218
212'
148
150
604
152
606
118
134
602
132
210
212
214
206
216
218
220
226
136
208
600

Fig. 7

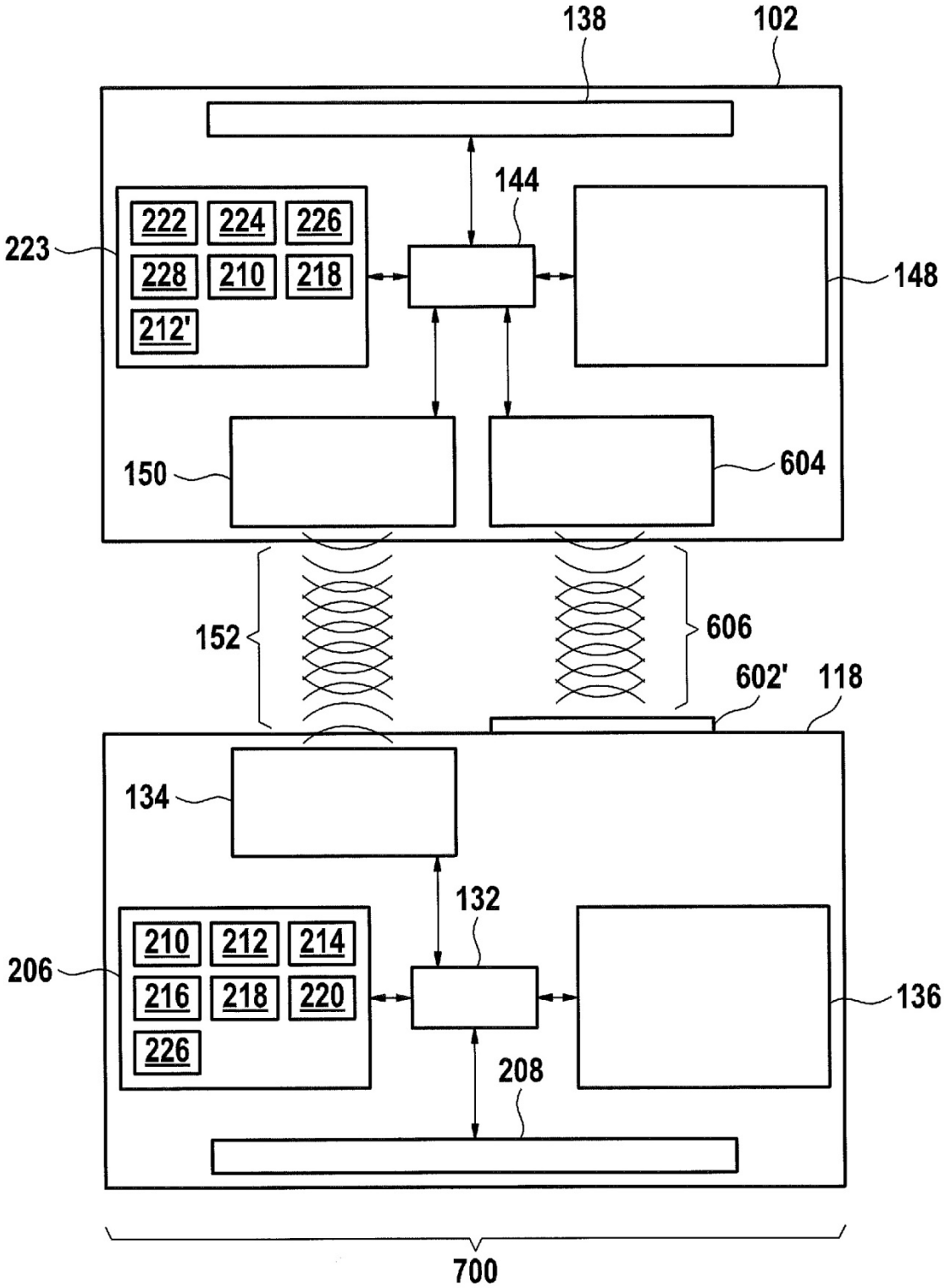

138
102
144
222
224
226
223
228
210
218
212'
148
150
604
152
606
602'
118
134
132
210
212
214
206
216
218
220
226
136
208
700

Fig. 8

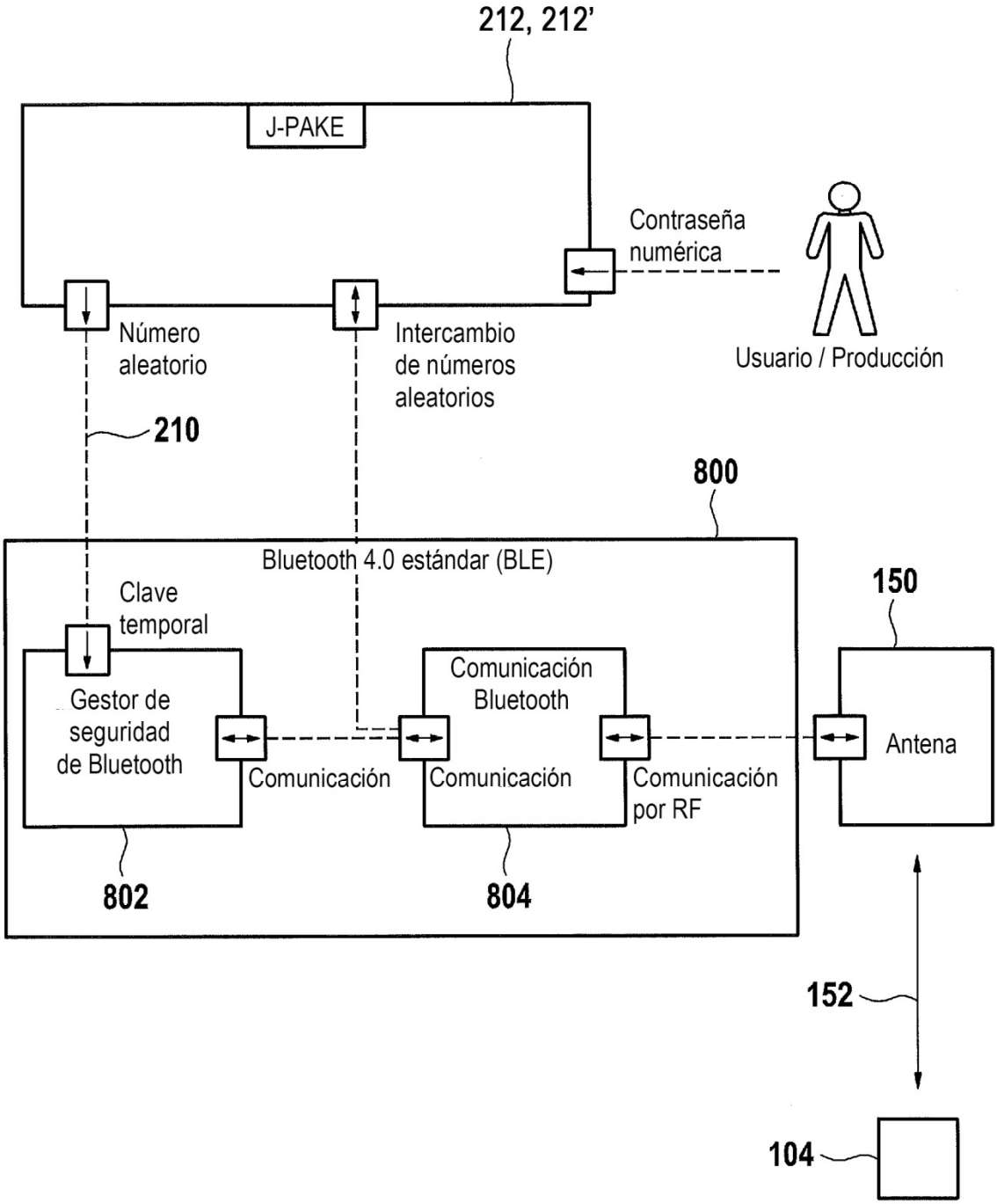
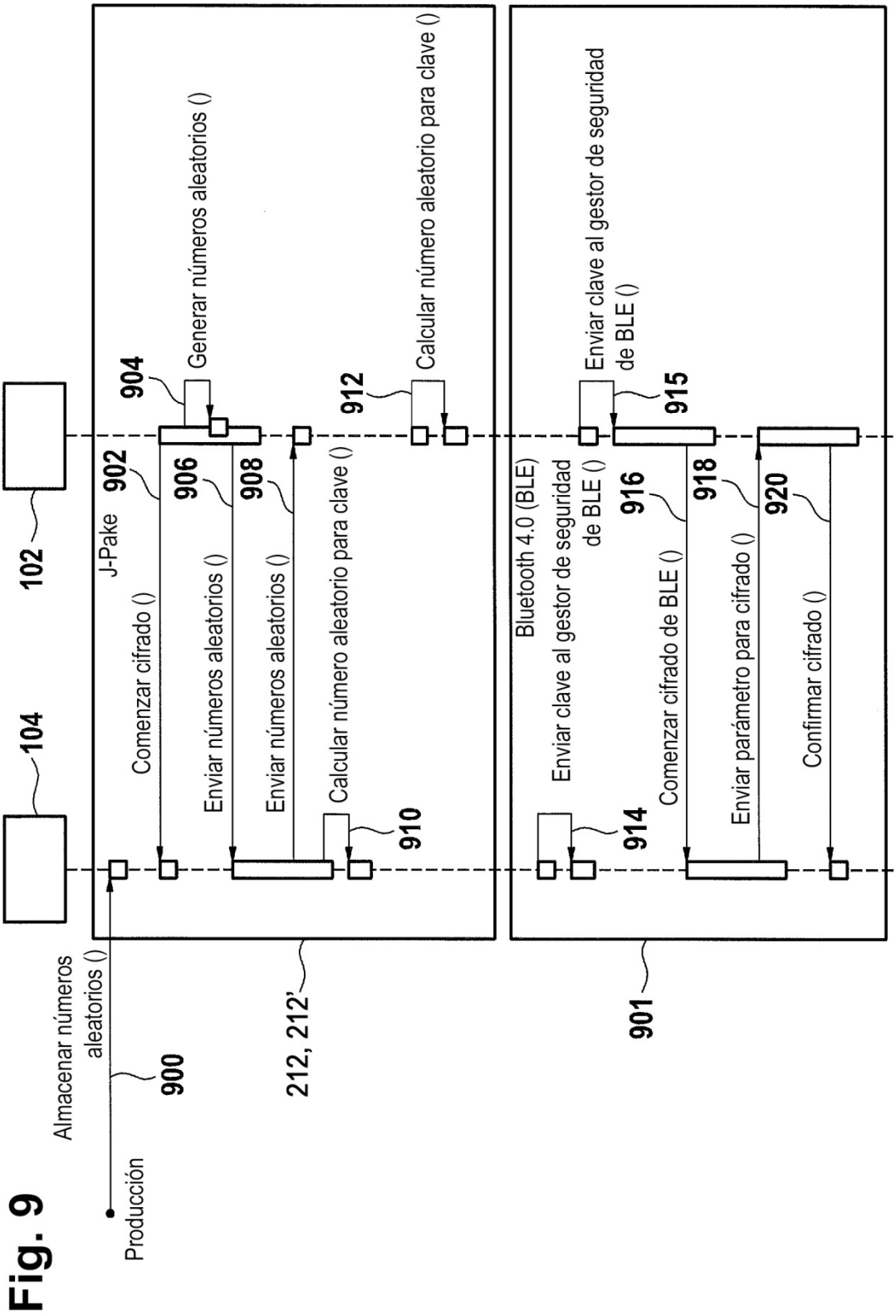

212, 212'
J-PAKE
Contraseña numérica
Usuario / Producción
Número aleatorio
Intercambio de números aleatorios
210
800
Bluetooth 4.0 estándar (BLE)
Clave temporal
Gestor de seguridad de Bluetooth
Comunicación
Comunicación Bluetooth
Comunicación
Comunicación por RF
150
Antena
802
804
152
104

Fig. 9


Producción
Almacenar números aleatorios ()
900
104
102
212, 212'
901
J-Pake
902
Comenzar cifrado ()
904
Generar números aleatorios ()
906
Enviar números aleatorios ()
908
Enviar números aleatorios ()
910
Calcular número aleatorio para clave ()
912
Calcular número aleatorio para clave ()
Bluetooth 4.0 (BLE)
914
Enviar clave al gestor de seguridad de BLE ()
915
Enviar clave al gestor de seguridad de BLE ()
916
Comenzar cifrado de BLE ()
918
Enviar parámetro para cifrado ()
920
Confirmar cifrado ()