(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 684 076**

(51) Int. CI.:

***G06F 21/34*** (2013.01)
***G06F 19/00*** (2008.01)
***G06F 21/57*** (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **23.10.2014 PCT/US2014/062013**

(87) Fecha y número de publicación internacional: **30.04.2015 WO15061595**

(96) Fecha de presentación y número de la solicitud europea: **23.10.2014 E 14792977 (2)**

(97) Fecha y número de publicación de la concesión europea: **16.05.2018 EP 3031002**

(54) Título: **Sistema de llave de hardware para protección de dispositivos**

(30) Prioridad:

**25.10.2013 US 201361895924 P**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
**01.10.2018**

(73) Titular/es:

**ASCENSIA DIABETES CARE HOLDINGS AG (100.0%)**
**Peter-Merian Strasse 90**
**4052 Basel, CH**

(72) Inventor/es:

**REYNOLDS, JEFFERY S.**

(74) Agente/Representante:

**LEHMANN NOVO, María Isabel**

## DESCRIPCIÓN

Sistema de llave de hardware para protección de dispositivos.

Campo de la invención

La presente invención se refiere, en general, a sistemas y métodos para proteger software, firmware, y/u otros datos almacenados en un dispositivo y, más concretamente, a sistemas y métodos que requieren que una llave de hardware se acople a un dispositivo médico antes de que pueda accederse al software, firmware y/u otros datos almacenados en el dispositivo médico por otro dispositivo.

Antecedentes de la invención

La determinación cuantitativa de analitos en fluidos corporales es de gran importancia en el diagnóstico y mantenimiento de ciertas condiciones fisiológicas. Por ejemplo, las personas con diabetes comprueban, con frecuencia, el nivel de glucosa en sus fluidos corporales. Los resultados de dichas pruebas pueden usarse para regular la entrada de glucosa en sus dietas y/o para determinar si la insulina u otra medicación necesita administrarse.

Muchos sistemas de diagnóstico emplean un medidor para calcular el valor de la glucosa en una muestra de sangre de una persona. Dichos medidores funcionan mediante la medición de una salida como, por ejemplo, corriente o color, de una reacción con la glucosa en la muestra. Los resultados de la prueba se muestran y almacenan, normalmente, por el medidor. Los medidores almacenan software, firmware y/u otros datos a los que puede accederse por un procesador para llevar a cabo mediciones y/o proveer otras funciones para el medidor.

La Solicitud de Patente Europea EP 2535830 describe un dispositivo médico que comprende un sensor de prueba y un puerto de sensor de prueba para determinar una concentración de analitos en una muestra provista en el sensor de prueba y una interfaz de comunicación que define un trayecto de comunicación para permitir comunicaciones entre el dispositivo médico y un dispositivo externo. Una rutina de autenticación de usuario evita el acceso no autorizado a los datos almacenados en el dispositivo médico.

La Solicitud de Patente de Estados Unidos US 2008/0244717 describe un sistema y método para confirmar la identidad y autoridad por un dispositivo médico de paciente.

Compendio de la invención

Las realizaciones descritas en la presente memoria proveen sistemas y métodos para proteger software, firmware y/u otros datos (a los que también se hace referencia, en su conjunto, en la presente memoria, como "datos") almacenados en un dispositivo médico como, por ejemplo, un medidor de glucosa en sangre. Según los aspectos de la presente invención, los sistemas y métodos requieren que una llave de hardware se acople físicamente a un dispositivo médico antes de que pueda accederse a los datos almacenados en el dispositivo médico por un dispositivo externo. La llave de hardware protege los datos en el dispositivo médico del acceso no autorizado. Algunas realizaciones pueden emplear una llave de hardware en un proceso que permite que un dispositivo externo actualice, mejore, añada y/o elimine datos almacenados en el dispositivo médico. Dicho proceso de modificación puede llevarse a cabo durante la fabricación del dispositivo médico o cuando el dispositivo médico se devuelve al fabricante para el mantenimiento. Dicho proceso de modificación puede también llevarse a cabo cuando el dispositivo médico está en el terreno, a saber, en posesión de un usuario. Como tal, el proceso de modificación permite a un fabricante administrar las características del dispositivo médico y asegurar que el dispositivo médico funciona de manera adecuada sin requerir que el usuario envíe el dispositivo médico físicamente otra vez al fabricante.

Según los aspectos de la presente invención, por ejemplo, los sistemas y métodos emplean un dispositivo médico y una llave de hardware. El dispositivo médico incluye al menos un dispositivo de memoria que almacena datos; una interfaz de comunicación que define un primer trayecto de comunicación para permitir las comunicaciones entre el dispositivo médico y un dispositivo externo o red; y una interfaz de llave de hardware que define un segundo trayecto de comunicación que está separado del primer trayecto de comunicación. La llave de hardware se configura para acoplarse al medidor mediante el segundo trayecto de comunicación definido por la interfaz de llave de hardware. Los datos en el al menos un dispositivo de memoria no pueden modificarse a menos que la interfaz de llave de hardware se acople físicamente a la llave de hardware. El dispositivo médico puede incluir un detector configurado para detectar la llave de hardware acoplada a la interfaz de llave de hardware. La llave de hardware puede incluir un componente de código de llave y líneas de conducción, donde la interfaz de llave de hardware recibe el código de llave mediante las líneas de conducción y los datos en el al menos un dispositivo de memoria no pueden modificarse a menos que el código de llave provisto por la llave de hardware se valide.

En algunas realizaciones, el dispositivo médico es un medidor que determina una concentración de analitos en una muestra provista en un sensor de prueba. El medidor incluye un puerto de sensor de prueba para recibir el sensor de

prueba, y el puerto de sensor de prueba actúa como la interfaz de llave de hardware. En algunos casos, el medidor además comprende múltiples contactos configurados para conectarse con electrodos en el sensor de prueba y recibir, mediante los electrodos, una señal electroquímica de una reacción entre un reactivo y la muestra en el sensor de prueba. La señal electroquímica indica la concentración de analitos. Además, los múltiples contactos pueden configurarse para conectarse con líneas de conducción en el sensor de prueba y recibir, mediante las líneas de conducción, un código de calibración correspondiente a la reacción entre el reactivo y la muestra en el sensor de prueba. Los múltiples contactos se configuran además para recibir un código de llave de la llave de hardware, donde los datos en el al menos un dispositivo de memoria no pueden modificarse a menos que el código de llave provisto por la llave de hardware se valide.

La invención se define por las reivindicaciones anexas.

Breve descripción de los dibujos

La Figura 1 ilustra un sistema a modo de ejemplo que incluye un dispositivo médico, un dispositivo informático, y un servidor, los cuales se describen para demostrar aspectos de la presente invención.

La Figura 2A ilustra una llave de hardware a modo de ejemplo que se emplea con el dispositivo médico de la Figura 1, según aspectos de la presente invención.

La Figura 2B además ilustra la llave de hardware a modo de ejemplo y dispositivo médico de la Figura 2A, según aspectos de la presente invención.

La Figura 3 ilustra un método a modo de ejemplo para emplear la llave de hardware y medidor de las Figuras 2A-B, según aspectos de la presente invención.

La Figura 4 ilustra otra llave de hardware a modo de ejemplo que se emplea con un dispositivo médico, según aspectos de la presente invención.

La Figura 5 ilustra incluso otra llave de hardware a modo de ejemplo que se emplea con un dispositivo médico, según aspectos de la presente invención.

Descripción

Las realizaciones descritas en la presente memoria proveen sistemas y métodos para proteger software, firmware y/u otros datos (a los que también se hace referencia, en su conjunto, en la presente memoria, como "datos") almacenados en un dispositivo médico como, por ejemplo, un medidor de glucosa en sangre. Según aspectos de la presente invención, los sistemas y métodos requieren que una llave de hardware se acople físicamente a un dispositivo médico antes de que pueda accederse a los datos almacenados en el dispositivo médico por un dispositivo externo. La llave de hardware protege los datos en el dispositivo médico del acceso no autorizado. Algunas realizaciones pueden emplear una llave de hardware en un proceso que permite que un dispositivo externo actualice, mejore, añada y/o elimine datos almacenados en el dispositivo médico. Dicho proceso de modificación puede llevarse a cabo durante la fabricación del dispositivo médico o cuando el dispositivo médico se devuelve al fabricante para el mantenimiento. Dicho proceso de modificación puede también llevarse a cabo cuando el dispositivo médico está en el terreno, a saber, en posesión de un usuario. Como tal, el proceso de modificación permite a un fabricante administrar las características del dispositivo médico y asegurar que el dispositivo médico funciona de manera adecuada sin requerir que el usuario envíe el dispositivo médico físicamente otra vez al fabricante.

Con referencia a la Figura 1, se describe un medidor 100 para ilustrar aspectos de la presente invención. Como se muestra en la Figura 1, el medidor 100 recibe un sensor de prueba 110 en un puerto de sensor de prueba 101. El sensor de prueba 110 se configura para recibir una muestra de fluidos, que es un analito que se analiza por el medidor 100. En aras de la descripción, el medidor 100 en el presente ejemplo es un medidor de glucosa en sangre que provee mediciones de un punto en el tiempo de concentraciones de glucosa en sangre en muestras de sangre recibidas en el sensor de prueba 110.

Como se muestra en la Figura 1, el sensor de prueba 110 puede ser un sensor de prueba electroquímico. Como tal, el sensor de prueba 110 incluye un área de recepción 111 que contiene un reactivo que reacciona con la muestra para proveer información relacionada con un analito en la muestra, a saber, concentración de glucosa en sangre. De manera específica, el reactivo convierte la glucosa en la muestra en una especie química que es electroquímicamente medible y refleja la concentración de glucosa en la muestra. El sensor de prueba 110 también incluye múltiples electrodos 112 que transmiten la señal eléctrica medible de la reacción electroquímica.

Por consiguiente, el medidor 100 incluye contactos 102a que hacen contacto con los electrodos 112 en el sensor de prueba 110 para recibir la señal eléctrica de los electrodos 112. El medidor 100 emplea un componente de procesamiento 103 para procesar la señal eléctrica y determinar una medición de concentración de glucosa. El

componente de procesamiento 103, por ejemplo, puede incluir un extremo frontal analógico que interactúa con los contactos 102 para recibir una señal analógica del sensor de prueba 110 y un motor digital de extremo posterior para procesar digitalmente la señal. El componente de procesamiento 103 incluye uno o más procesadores de ordenador que ejecutan instrucciones programadas según un algoritmo de medición. Las instrucciones programadas se almacenan en, y se leen de, al menos un dispositivo de memoria 104. El dispositivo de memoria 104, por ejemplo, puede incluir cualquier tipo o combinación de dispositivos de almacenamiento grabables y legibles por ordenador. Por ejemplo, el dispositivo de memoria 104 puede ser una memoria permanente como, por ejemplo, una memoria flash, o similares.

En general, el componente de procesamiento 103 puede ejecutar instrucciones programadas almacenadas como datos en el dispositivo de memoria 104. Las instrucciones programadas proveen varias funciones para el medidor 100 y controlan varios aspectos del funcionamiento del medidor 100. Por ejemplo, el medidor 100 puede incluir una interfaz de usuario 105 que provee una interfaz gráfica de usuario (GUI, por sus siglas en inglés) 105a y controles operados por el usuario 105b. La visualización 105a puede presentar información relacionada con los resultados de la prueba, el procedimiento de prueba, etc., así como otras respuestas a entradas de usuario, etc. Por consiguiente, el componente de procesamiento 103 puede ejecutar instrucciones programadas para mostrar información en la GUI 105a.

El dispositivo de memoria 104 también puede almacenar parámetros de programas, constantes, tablas de consulta, etc., que se emplean por el componente de procesamiento 103 cuando se ejecutan las instrucciones programadas. Los parámetros del programa, por ejemplo, pueden alterar el funcionamiento del medidor 100 según consideraciones geográficas o de mercado. En general, el dispositivo de memoria 104 almacena software, firmware y otros datos que se usan para el funcionamiento del medidor 100.

Como se muestra en la Figura 1, el medidor 100 puede acoplarse, de manera comunicativa, a un dispositivo informático externo 200 mediante una conexión cableada o inalámbrica 10. El dispositivo informático 200 puede ser un ordenador de sobremesa u ordenador personal portátil, un ordenador personal portable o de bolsillo, una tableta, un teléfono/dispositivo inteligente, un asistente de datos personal (PDA, por sus siglas en inglés), o cualquier otro dispositivo que incluya capacidades de procesamiento y otras características que puedan emplearse con el medidor 100. Aunque el medidor 100 puede ejecutar un procedimiento de prueba para producir resultados de prueba y presentar información relacionada en la GUI 105a, el dispositivo informático 200 puede proveer una funcionalidad más avanzada para la gestión, procesamiento y visualización de los resultados de prueba e información relacionada. Por ejemplo, el dispositivo informático 200 tiene las capacidades de potencia de procesamiento, memoria de programa (p.ej., RAM) y visualización necesarias para ejecutar software de gestión de datos de salud que provee un análisis y presentación más avanzados de los resultados de prueba medidos por el medidor 100. Por ejemplo, el dispositivo informático 200 puede descargar resultados de prueba del medidor 100, llevar a cabo un análisis estadístico complejo de los resultados de prueba, y mostrar el análisis estadístico como gráficos en una GUI de alta resolución provista por el dispositivo informático 200.

Como se muestra en la Figura 1, el medidor 100 incluye una interfaz de comunicación 106 que permite al medidor 100 conectarse por cable al dispositivo informático 200, por ejemplo, mediante un Bus Universal en Serie (USB, por sus siglas en inglés), RS-232, colector abierto u otro protocolo. La interfaz de comunicación 106, por ejemplo, puede conectarse directamente al dispositivo informático 200, p.ej., a un puerto USB, o puede recibir un cable de comunicación que se extiende entre el medidor 100 y el dispositivo informático 200. De manera alternativa o adicional, el medidor 100 puede comunicarse, de forma inalámbrica, con el dispositivo informático 200, por ejemplo, mediante un enlace de radiofrecuencia (RF) (p.ej., telemetría RF de corto alcance) como, por ejemplo, tecnologías inalámbricas Bluetooth®, Zigbee, tecnología Z-Sense™, FitSense, sistema BodyLAN™ y otras tecnologías RF. Otras tecnologías de comunicación inalámbricas como, por ejemplo, enlaces infrarrojos (IR), también pueden usarse. En general, la conexión cableada o inalámbrica 10 emplea cualquier tecnología que permita que los datos se intercambien entre el medidor 100 y el dispositivo informático 200.

El dispositivo informático 200 puede, a su vez, acoplarse, de manera comunicativa, a otros sistemas externos en una red como, por ejemplo, Internet, una red de área local/amplia (LAN/WAN, por sus siglas en inglés), una red en la nube, una red celular, etc. Por ejemplo, el dispositivo informático 200 puede acoplarse a la red mediante una conexión cableada, p.ej., conexión Ethernet, o una conexión inalámbrica, p.ej., mediante Wi-Fi como, por ejemplo, una zona de acceso inalámbrico de banda ancha. Los sistemas externos pueden proveer otras funciones para el medidor 100. Por ejemplo, el dispositivo informático 200 puede acceder a un sistema de salud a distancia que permite al medidor 100 compartir resultados de prueba con profesionales del sector de la salud u otros sistemas de diagnóstico en ubicaciones remotas. Como se muestra en la Figura 1, el dispositivo informático 200 se acopla, de manera comunicativa, mediante una conexión cableada o inalámbrica 20, a un sistema de servidor 300 que se asocia al fabricante del medidor 100 (o tercero autorizado). Como tal, el medidor 100 puede intercambiar datos con el fabricante del medidor 100. En realizaciones alternativas, el medidor 100 puede acoplarse, de manera comunicativa, al sistema de servidor 300 sin el dispositivo informático 100. En algunos casos, el medidor 100 está equipado para conectarse a una red para comunicarse con el sistema de servidor 300. En otros casos, el medidor

100 puede conectarse, de forma local, con el sistema de servidor 300, por ejemplo, durante la fabricación o cuando el medidor se devuelve al fabricante para el mantenimiento.

Se comprende que la arquitectura de comunicación ilustrada en la Figura 1 se provee meramente como un ejemplo para ilustrar aspectos de la presente invención. Las tecnologías y redes cableadas o inalámbricas descritas más arriba también se proveen solo como ejemplos. En general, según aspectos de la presente invención, cualquier dispositivo médico puede incluir una interfaz de comunicación que emplea cualquier combinación de tecnologías cableadas y/o inalámbricas para permitir que los datos se intercambien entre el dispositivo médico y uno o más dispositivos externos, los cuales pueden o pueden no residir en una o más redes.

Según se describe más arriba, el dispositivo de memoria 104 del medidor 100 almacena software, firmware y/u otros datos requeridos para el cálculo de los resultados de prueba y funcionamiento del medidor 100. En algunos casos, los datos en el dispositivo de memoria 104 pueden actualizarse, o parchearse, con versiones más nuevas para enmendar errores/errores de programación y para asegurar que el medidor 100 funciona de manera adecuada. En otros casos, los datos en el dispositivo de memoria 104 pueden modificarse para actualizar, reconfigurar o personalizar las características provistas por el medidor 100. En incluso otros casos, los datos pueden añadirse al dispositivo de memoria 104 para proveer nuevas características en el medidor 100 y, de esta manera, hacer que las últimas características estén disponibles para usuarios que ya poseen el medidor 100. En otros casos, pueden emplearse nuevos datos para hacer que el medidor 100 existente sea compatible con otros accesorios o dispositivos recientemente lanzados. Por ejemplo, si el medidor 100 usa un sensor de prueba para pruebas de sangre para verificar la concentración de glucosa en sangre y el fabricante desarrolla un sensor de prueba nuevo que mejora la exactitud o el tiempo de prueba, las realizaciones permitirían al usuario mejorar los datos de modo que el medidor 100 puede leer el nuevo sensor de prueba. Por consiguiente, al permitir que el medidor 100 se comunique con el sistema de servidor 300 del fabricante, el fabricante puede actualizar, mejorar, añadir y/o eliminar los datos almacenados en el dispositivo de memoria 104 incluso si el dispositivo médico 100 ya se encuentra en posesión del usuario.

El sistema de servidor 300 del fabricante almacena códigos y/u otros datos que pueden transmitirse, p.ej., en las conexiones 10, 20, al medidor 100. Los programas en el sistema de servidor 300, dispositivo informático 200, medidor 100, o cualquier combinación de ellos, pueden gestionar aspectos del proceso de modificación. De manera ventajosa, el proceso de modificación puede activarse y llevarse a cabo de forma electrónica en un proceso de autoservicio en línea que no requiere que el usuario contacte al fabricante para una asistencia personal directa. Por ejemplo, si una agencia regulatoria gubernamental requiere una rellamada del medidor 100 para corregir un problema, los usuarios pueden corregir el problema por sí mismos a través del proceso de autoservicio en línea sin tener que enviar el medidor 100 al fabricante.

La comunicación entre el medidor 100 y el sistema de servidor 300 se describe en la presente memoria para ilustrar aspectos de la presente invención. En general, se comprende que los aspectos de la presente invención pueden emplearse cuando cualquier dispositivo médico se acopla, de manera comunicativa, a cualquier dispositivo externo, que puede o puede no residir en una o más redes.

Debido a las importantes funciones médicas asociadas al medidor 100, las realizaciones pueden emplear procedimientos de validación para asegurar que el proceso de modificación no ha corrompido los datos almacenados en el medidor 100 y que el medidor 100 funciona de manera adecuada. Para una seguridad adicional de los datos, la entrada de ID/contraseñas de usuarios, números de identificación personal (PIN, por sus siglas en inglés) y/u otros códigos de autorización pueden requerirse para iniciar el proceso de modificación. Además, el proceso de modificación puede emplear técnicas de encriptación/desencriptación para el intercambio de datos entre el medidor 100 y el servidor de sistema 300.

Aunque las técnicas digitales pueden emplearse para añadir cierta seguridad a las comunicaciones entre un medidor y un dispositivo externo, p.ej., el sistema de servidor 300 en una red, el medidor puede ser susceptible al acceso digital y modificación no autorizada o corrupción de datos almacenados en el medidor. Aunque las capacidades de conectividad del medidor pueden proveer características beneficiosas como, por ejemplo, aquellas descritas más arriba, la conectividad puede dejar el medidor abierto a una manipulación no autorizada o corrupción si las técnicas de seguridad digital fallan. Los aspectos de la presente invención, sin embargo, minimizan la susceptibilidad de los dispositivos médicos a dicha manipulación o corrupción.

En particular, los aspectos de la presente invención requieren que una llave de hardware se acople físicamente a un dispositivo médico antes de que se otorgue acceso a sus datos. La conexión física entre la llave de hardaware y el dispositivo médico en general requiere el acceso físico local al dispositivo médico y no puede falsificarse digitalmente. Por ejemplo, las Figuras 2A-B ilustran una llave de hardware 400 que puede combinarse con el medidor 100. En particular, la llave de hardware 400 se configura para recibirse por el puerto 101 que normalmente recibe sensores de prueba 110, según se muestra en la Figura 1. La llave de hardware 400 tiene una forma y dimensiones que son suficientemente similares al sensor de prueba 110 para permitir la compatibilidad con el puerto 101.

Como la Figura 2B ilustra de manera más clara, la llave de hardware 400 incluye un componente de código de llave 401 y múltiples líneas de conducción 402. El componente de código de llave 401 provee un conjunto preprogramado (estático o dinámico) de señales que se transmiten al medidor 100 mediante las líneas de conducción 402. Cuando la llave de hardware 400 se recibe en el puerto 101, los contactos 102a del medidor 100 pueden conectarse con las líneas de conducción 402 para recibir las señales del componente de código de llave 401. Además de tener contactos 102a que pueden recibir señales analógicas de la reacción electroquímica en el sensor de prueba 110, el medidor 100 puede también incluir contactos adicionales 102b para recibir códigos de calibración de líneas de conducción en el sensor de prueba 110. Los códigos de calibración calibran el algoritmo de medición para representar variaciones en el reactivo que se usan en los sensores de prueba 110. Cualquier combinación de los contactos 102a o 102b puede usarse para conectarse con las líneas de conducción 402 de la llave de hardware 400. La conexión conductiva entre el medidor 100 y la llave de hardware 400 también permite al componente electrónico 401 extraer energía eléctrica necesaria de una fuente de alimentación en el medidor 100, p.ej., una batería.

El medidor 100 puede detectar la llave de hardware 400 cuando se inserta en el puerto 101. Como se muestra en la Figura 2B, el medidor 100 incluye un detector 107 para detectar el sensor de prueba 110 cuando se recibe en el puerto 101. El detector 107 puede emplearse, de forma similar, para detectar la llave de hardware 400 cuando se recibe en el puerto 101. Mientras la llave de hardware 400 se mueve hacia el puerto 101, la llave de hardware 400 puede hacer contacto con un componente móvil conductivo 107a del detector 107. En respuesta, el componente móvil conductivo 107a se mueve, p.ej., pivota, para cerrar un circuito eléctrico en el medidor 100 y, de esta manera, señalizar la presencia de la llave de hardware 400 y permitir el acceso a los datos almacenados en el dispositivo de memoria 104. Además, las líneas de conducción 402 de la llave de hardware 400 pueden conectarse con los contactos 102a y/o contactos 102b del medidor 100 para cerrar un circuito eléctrico específico que identifica, de manera única, la llave de hardware 400 y distingue la llave de hardware 400 de un sensor de prueba 110.

Como se ilustra en la realización a modo de ejemplo de la Figura 3, la comunicación se establece en la función 502 entre el medidor 100 y el sistema de servidor 300 en una red u otra conexión. En algunos casos, por ejemplo, el medidor 100 puede comunicarse con el sistema de servidor 300 mediante el dispositivo informático 200, como se muestra en la Figura 1. En otros casos, el medidor 100 puede comunicarse más directamente con el dispositivo informático 200. El proceso de modificación se inicia entonces en la función 504, p.ej., automáticamente después de establecer la comunicación en la función 502 o manualmente mediante el ingreso de una secuencia de comandos mediante el medidor 100, dispositivo informático 200 o sistema de servidor 300. La secuencia de comandos puede requerir la entrada de ID/contraseñas de usuario, números de identificación personal (PIN) y/u otros códigos de autorización para identificar el medidor 100 y establecer la autorización digital para el intercambio de datos entre el medidor 100 y el sistema de servidor 300. La secuencia de comandos puede ejecutarse de manera automática o manual. Antes de que se pueda acceder a y modificar datos almacenados en el medidor 100, sin embargo, el medidor 100 en la función 506 también debe detectar la llave de hardware 400 en el puerto 101. En la realización de la Figura 3, la llave de hardware 400 se usa en combinación con técnicas de seguridad digital, p.ej., entrada de ID/contraseñas de usuario, etc. Además, el conjunto preprogramado correcto de señales del componente de código de llave 401 debe transmitirse al medidor 100 en la función 508. La llave de hardware 400 debe acoplarse físicamente al medidor 100 antes de que se permita que el proceso de modificación proceda. Con el fin de añadir seguridad adicional, una negociación adicional u otros intercambios entre el medidor 100 y el sistema de servidor 300 pueden requerirse en la función 510 opcional. Una vez que el medidor 100 se ha identificado de manera apropiada y se ha permitido el acceso al medidor 100 con la llave de hardware 400, las modificaciones, p.ej., actualizaciones, mejoras y/o adiciones, se identifican/seleccionan en la función 512. Y los datos almacenados en el dispositivo de memoria 104 del medidor 100 se modifican, por consiguiente, en la función 514. En algunos casos, las modificaciones se ejecutan de manera automática, p.ej., para enmiendas de errores de programación cruciales o actualizaciones de cumplimiento de las normas. En otros casos, las modificaciones se ejecutan solo después de la aprobación del usuario, p.ej., para características de conveniencia opcionales. Un programa de gestión de versión puede emplearse para determinar qué software, firmware y/u otros datos en el medidor 100 son compatibles con, y pueden reemplazarse por, versiones más nuevas o diferentes almacenadas en el sistema de servidor 300.

En algunas realizaciones, los datos B del sistema de servidor 300 se descargan en un área del dispositivo de memoria 104 que está separada del área que almacena los datos A preexistentes empleados por el medidor 100. Un área de memoria puede estar específicamente dedicada al proceso de modificación. En otras palabras, los datos A se retienen, antes que eliminarse o sobrescribirse, al menos hasta que la descarga completa de los datos B se haya verificado y la verificación del sistema de validación se haya completado de manera exitosa. Si la descarga y la verificación del sistema son exitosas, los datos B se despliegan para el funcionamiento regular. Si la descarga y la verificación del sistema no son exitosas, sin embargo, los datos A aún se encuentran disponibles y proveen una opción de recuperación o restablecimiento. Los datos B se retiran cuando el proceso de modificación falla. En algunas realizaciones, los datos A se retienen incluso después de que los datos B se despliegan para dar a los usuarios la opción de restablecer los datos A.

Al permitir que la llave de hardware 400 se reciba en el puerto 101, como se muestra en las Figuras 1B y 1C, las realizaciones de más arriba proveen una solución particularmente rentable y conveniente. El medidor 100 no tiene que reconfigurarse estructuralmente para alojar la llave de hardware 400. Mediante el uso del puerto 101, las

realizaciones toman ventaja de componentes que ya existen en el diseño de medidor original, p.ej., los contactos 102a, los contactos 102b, el detector 107, etc. No se requieren cambios en los diseños de hardware de medidor existentes. Además, el puerto 101 para la llave de hardware 400 establece un trayecto de comunicación con el medidor 100 que está separado de las comunicaciones mediante el elemento de interfaz 106.

Según se describe más arriba, el componente de código de llave 401 provee un conjunto preprogramado (estático o dinámico) de señales de código de llave que se transmiten al medidor 100 mediante las líneas de conducción 402. El componente de código de llave 401 puede ser cualquier dispositivo que provee un código de llave que puede transmitirse al medidor 100 para identificar la llave de hardware 400. En una realización, las líneas de conducción 402 en la llave de hardware 400 pueden configurarse como el sensor de prueba 110 de modo que pueden comunicar un código de calibración específico (no usado con el sensor de prueba 110) a los contactos 102b como un código de llave estático. O en otra realización, la llave de hardware 400 puede funcionar en ciclos a través de una serie de códigos de calibración para proveer un código de llave diferente (dinámico) a los contactos 102b cada vez que se interroga. O en incluso otra realización, las líneas de conducción 402 en la llave de hardware 400 pueden producir una resistencia dentro de un rango fijo que se transmite a los contactos 102a como el código de llave; dicho sistema puede emplearse con medidores 100 que no incluyen contactos 102b para recibir códigos de calibración o un detector 107. En general, las realizaciones pueden usar cualquier combinación de los contactos 102a y 102b para recibir cualquier combinación de códigos de calibración estáticos o dinámicos, señales de resistencia analógicas, etc., como códigos de llave de la llave de hardware 400.

Se comprende que otras realizaciones pueden emplear otros enfoques para acoplar la llave de hardware al dispositivo médico. En general, para recibir un código de llave de hardware, los aspectos de la presente invención pueden emplear cualquier entrada/interfaz analógica o digital que esté separada del trayecto de comunicación a redes o dispositivos externos. Por ejemplo, como se muestra en la Figura 4, un medidor 600 se acopla, de manera comunicativa, a un teléfono inteligente 700 mediante una conexión inalámbrica o cableada 30, p.ej., mediante el uso de una interfaz de comunicación 606. Mientras el teléfono inteligente 700 provee conectividad inalámbrica a una red, p.ej., red Wi-Fi, red celular, etc., este provee otro trayecto de comunicación para transmitir un código de llave al medidor 600. Por ejemplo, el teléfono inteligente 700 incluye una entrada (enchufe hembra) de micrófono 701 que puede emplearse para recibir una llave de hardware 800 que provee un código de llave analógico. La llave de hardware 800 puede incluir un componente de código de llave 801 que determina un código de llave que se transmite al teléfono inteligente 700 mediante un conector 802 y luego al medidor 600. La entrada analógica a través de la entrada de micrófono 701 asegura que el código de llave no puede falsificarse digitalmente de forma remota. De manera ventajosa, la realización de la Figura 4 toma ventaja de componentes que ya existen en el medidor original y diseños de teléfonos inteligentes. El diseño de hardware original del medidor 600 y el teléfono inteligente 700 no tienen que modificarse.

Se comprende también que las realizaciones no se encuentran limitadas al uso de hardware existente para emplear aspectos de la presente invención. Por ejemplo, como se muestra en el ejemplo de la Figura 5, antes que usar un puerto de sensor de prueba 901 para recibir una llave de hardware 1000, un medidor 900 incluye un puerto de llave adicional 908 que se configura específicamente para recibir la llave de hardware 1000. La llave de hardware 1000 puede ser similar a la llave de hardware 400 descrita más arriba. Por ejemplo, la llave de hardware 1000 puede incluir un componente de código de llave 1001 que determina un código de llave que se transmite al medidor 900 mediante líneas de conducción 1002. Como se muestra en la Figura 5, el medidor 900 también incluye una interfaz de comunicación 906. De manera similar a las realizaciones descritas más arriba, el puerto 908 para la llave de hardware 1000 establece un trayecto de comunicación con el medidor 900 que está separado de las comunicaciones mediante el elemento de interfaz 906.

En realizaciones alternativas, la llave de hardware puede integrarse físicamente, y más permanentemente acoplarse, al medidor. La llave de hardware y el medidor pueden funcionar de manera similar a las realizaciones de más arriba para proteger los datos en el medidor. En lugar de insertar la llave de hardware en un puerto, sin embargo, el trayecto de comunicación entre el medidor y la llave de hardware puede establecerse, por ejemplo, mediante el funcionamiento manual de un conmutador. La llave de hardware en dichas realizaciones alternativas puede incluir un componente de código de llave y líneas de conducción para transmitir un código de llave a otros circuitos de procesamiento en el medidor cuando la llave de hardware se enciende. El trayecto de comunicación entre el medidor y la llave de hardware está separado de otras interfaces de comunicación para el medidor.

Aunque los ejemplos de más arriba pueden describirse con respecto a un proceso de modificación que ocurre después de que los dispositivos médicos ya se encuentran en posesión de un usuario (a saber, en el terreno), el proceso de modificación puede llevarse a cabo durante la fabricación del dispositivo médico o cuando el dispositivo médico se devuelve al fabricante para el mantenimiento. En otras palabras, la llave de hardware debe acoplarse al dispositivo médico según se describe más arriba antes de que cualquier sistema de programación pueda transmitir software, firmware y/u otros datos a la memoria del dispositivo médico durante la fabricación.

En general, al requerir que una llave de hardware se acople físicamente a un dispositivo médico para permitir el acceso, los aspectos de la presente invención protegen la integridad del software, firmware y/u otros datos en el

dispositivo médico mientras aún permiten que el dispositivo médico se conecte a sistemas externos que pueden mejorar el uso del dispositivo médico. Antes que depender solamente de un proceso de modificación digital a través de una interfaz de comunicación convencional que conecta el medidor a sistemas externos, se requiere, además, que un puerto separado (un puerto de señal analógica o mixta) reciba la llave de hardware. En otras palabras, la comunicación con la llave de hardware no se asocia al acceso digital mediante la interfaz de comunicación convencional. De manera ventajosa, el requisito de llave de hardware previene el acceso no autorizado a datos en un dispositivo médico a lo largo de una red u otra conexión de comunicaciones, dado que incluso si la seguridad digital falla, no puede accederse a los datos en el medidor sin la llave de hardware y el acceso físico a los dispositivos médicos.

Aunque los medidores descritos en las realizaciones de más arriba pueden referirse a la medición de la concentración de glucosa, otras realizaciones pueden medir la concentración de otros analitos en la muestra de fluidos. Los analitos que pueden analizarse incluyen glucosa, perfil lipídico (p.ej., colesterol, triglicéridos, LDL y HDL), oligoalbúmina, hemoglobina $A_1C$, fructosa, lactato o bilirrubina. Los analitos pueden encontrarse en una muestra de sangre completa, una muestra de suero sanguíneo, una muestra de plasma sanguíneo, otros fluidos corporales como ISF (líquido intersticial) y orina, y fluidos no corporales. Además, se comprende que otros dispositivos médicos o dispositivos electrónicos no médicos pueden emplear aspectos de la presente invención para mantener la seguridad de los datos.

Mientras la invención es susceptible a varias modificaciones y formas alternativas, las realizaciones y métodos específicos de aquella se han mostrado a modo de ejemplo en los dibujos y se describen en detalle en la presente memoria.

**REIVINDICACIONES**

1. Un dispositivo médico (100), que comprende:

al menos un dispositivo de memoria (104) que almacena datos;

un puerto de sensor de prueba (101) para recibir un sensor de prueba (110);

una interfaz de comunicación (106) que define un primer trayecto de comunicación para permitir las comunicaciones entre el dispositivo médico (100) y un dispositivo externo (200) o red (10); y

una interfaz de llave de hardware configurada para recibir una llave de hardware (400), la interfaz de llave de hardware definiendo un segundo trayecto de comunicación que está separado del primer trayecto de comunicación, en donde el primer puerto de sensor (101) actúa como la interfaz de llave de hardware, y

en donde el dispositivo médico se configura para evitar que los datos en el al menos un dispositivo de memoria se modifiquen a menos que la interfaz de llave de hardware se acople físicamente a la llave de hardware,

en donde el dispositivo médico es un medidor que determina una concentración de analitos en una muestra provista en un sensor de prueba.

2. El dispositivo médico de la reivindicación 1, que además comprende:

múltiples contactos (102) configurados para conectarse con electrodos en el sensor de prueba y recibir, mediante los electrodos, una señal electroquímica de una reacción entre un reactivo y la muestra en el sensor de prueba, la señal electroquímica indicando la concentración de analitos, los múltiples contactos configurados además para recibir un código de llave de la llave de hardware, en donde los datos en el al menos un dispositivo de memoria no pueden modificarse a menos que el código de llave provisto por la llave de hardware se valide.

3. El dispositivo médico de la reivindicación 2, en donde la llave de hardware incluye líneas de conducción (402) que proveen una resistencia que se detecta por los múltiples contactos, la resistencia definiendo el código de llave.

4. El dispositivo médico de la reivindicación 1, que además comprende:

múltiples contactos configurados para conectarse con líneas de conducción en el sensor de prueba y recibir, mediante las líneas de conducción, un código de calibración correspondiente a la reacción entre un reactivo y la muestra en el sensor de prueba, los múltiples contactos configurados además para recibir un código de llave de la llave de hardware, en donde los datos en el al menos un dispositivo de memoria no pueden modificarse a menos que el código de llave provisto por la llave de hardware se valide.

5. El dispositivo médico de la reivindicación 1, que además comprende un detector (107) configurado para detectar la llave de hardware acoplada a la interfaz de llave de hardware.

6. El dispositivo médico de la reivindicación 1, en donde la llave de hardware incluye un componente de código de llave (1001) y líneas de conducción (1002), la interfaz de llave de hardware recibiendo el código de llave mediante las líneas de conducción y los datos en el al menos un dispositivo de memoria no pueden modificarse a menos que el código de llave provisto por la llave de hardware se valide.

7. Un sistema de dispositivo médico, que comprende:

un dispositivo médico de cualquiera de las reivindicaciones 1 a 6.

8. Un método para un sistema de dispositivo médico, que comprende:

establecer una conexión entre un dispositivo médico y una red o dispositivo externo mediante un primer trayecto de comunicación definido por una interfaz de comunicación;

iniciar un proceso de modificación, que incluye ejecutar una secuencia de comandos;

detectar un acoplamiento físico entre el dispositivo médico y una llave de hardware, la llave de hardware acoplada al dispositivo médico mediante un segundo trayecto de comunicación definido por una interfaz de llave de hardware, el segundo trayecto de comunicación estando separado del primer trayecto de comunicación, en donde el dispositivo médico incluye un puerto de sensor de prueba para recibir un sensor de prueba, y el puerto de sensor de prueba actúa como la interfaz de llave de hardware; y

modificar datos almacenados en al menos un dispositivo de memoria en el dispositivo médico según el proceso de modificación,

en donde el dispositivo médico se configura para evitar que los datos en el al menos un dispositivo de memoria se modifiquen a menos que la interfaz de llave de hardware se acople físicamente a la llave de hardware,

en donde el dispositivo médico es un medidor que determina una concentración de analitos en una muestra provista en un sensor de prueba.

9. El método de la reivindicación 8, que además comprende detectar un código de llave de la llave de hardware y validar el código de llave, en donde los datos en el al menos un dispositivo de memoria no pueden modificarse a menos que el código de llave provisto por la llave de hardware se valide.

10. El método de la reivindicación 8, en donde la ejecución de la secuencia de comandos incluye ingresar información de autorización.

11. El método de la reivindicación 8, en donde el medidor además comprende múltiples contactos configurados para conectarse con electrodos en el sensor de prueba y recibir, mediante los electrodos, una señal electroquímica de una reacción entre un reactivo y la muestra en el sensor de prueba, la señal electroquímica indicando la concentración de analitos, los múltiples contactos configurados además para recibir un código de llave de la llave de hardware, en donde los datos en el al menos un dispositivo de memoria no pueden modificarse a menos que el código de llave provisto por la llave de hardware se valide.

12. El método de la reivindicación 8, en donde el medidor además comprende múltiples contactos configurados para conectarse con líneas de conducción en el sensor de prueba y recibir, mediante las líneas de conducción, un código de calibración correspondiente a la reacción entre un reactivo y la muestra en el sensor de prueba, los múltiples contactos configurados además para recibir un código de llave de la llave de hardware, en donde los datos en el al menos un dispositivo de memoria no pueden modificarse a menos que el código de llave provisto por la llave de hardware se valide.

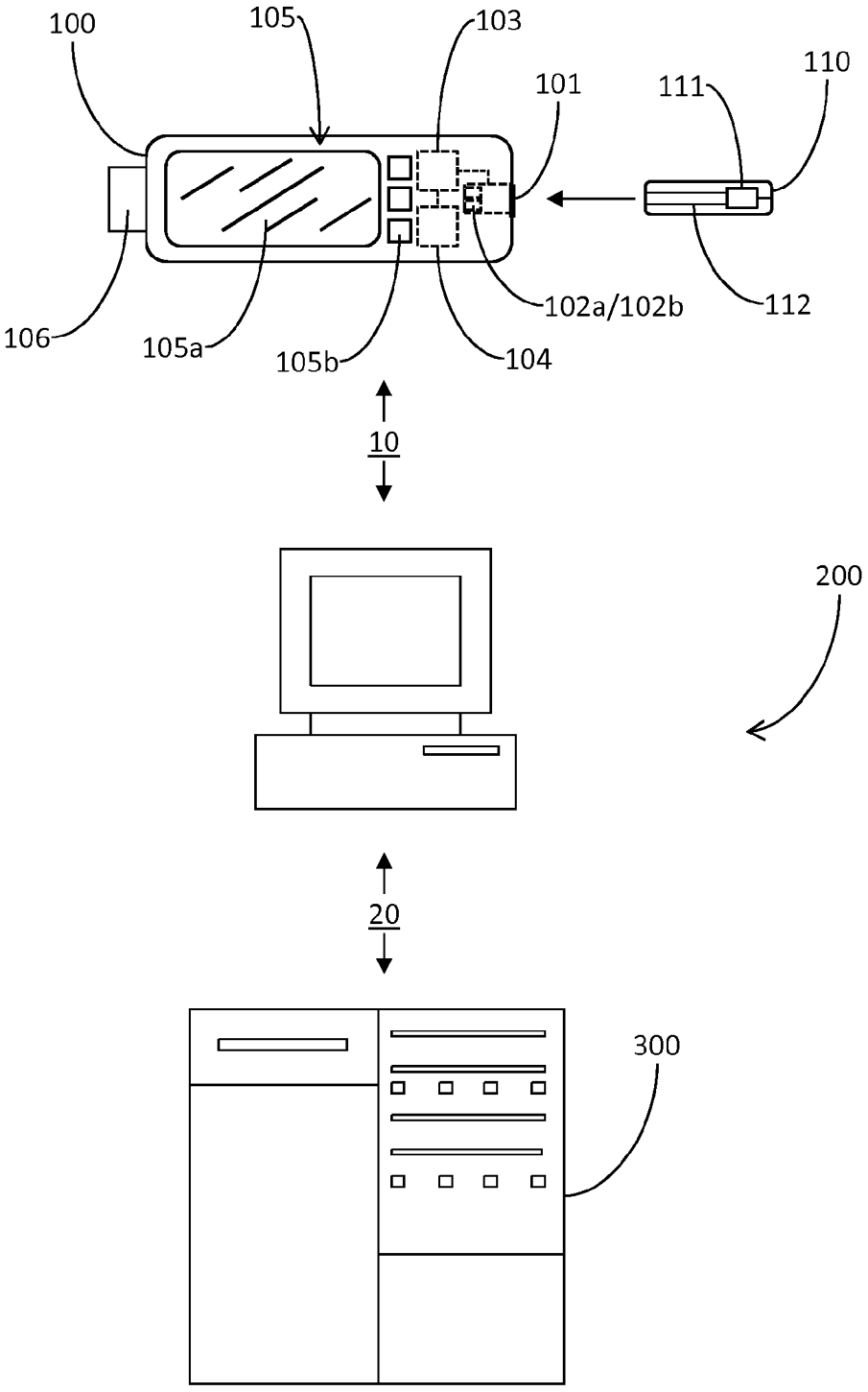
100
105
103
101
111
110
106
105a
105b
104
102a/102b
112
10
200
20
300

FIG. 1

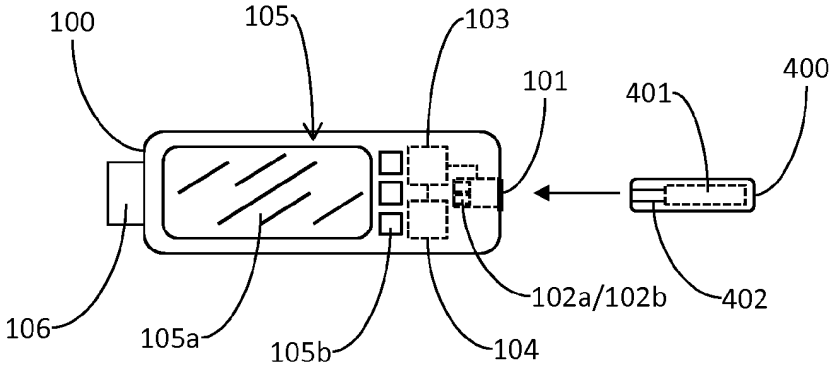
100
105
103
101
401
400
106
105a
105b
104
102a/102b
402

FIG. 2A

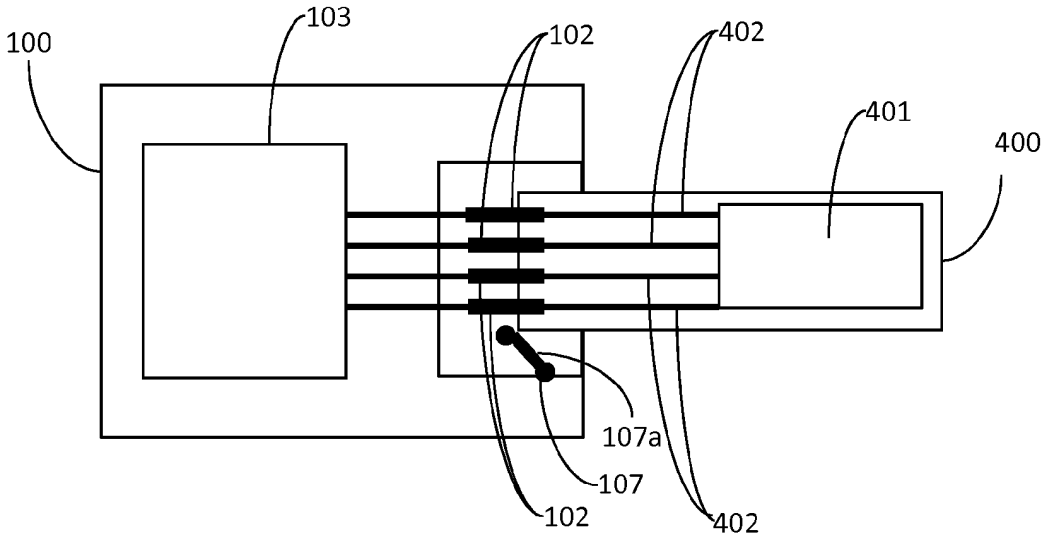
100
103
102
402
401
400
107a
107
102
402

FIG. 2B

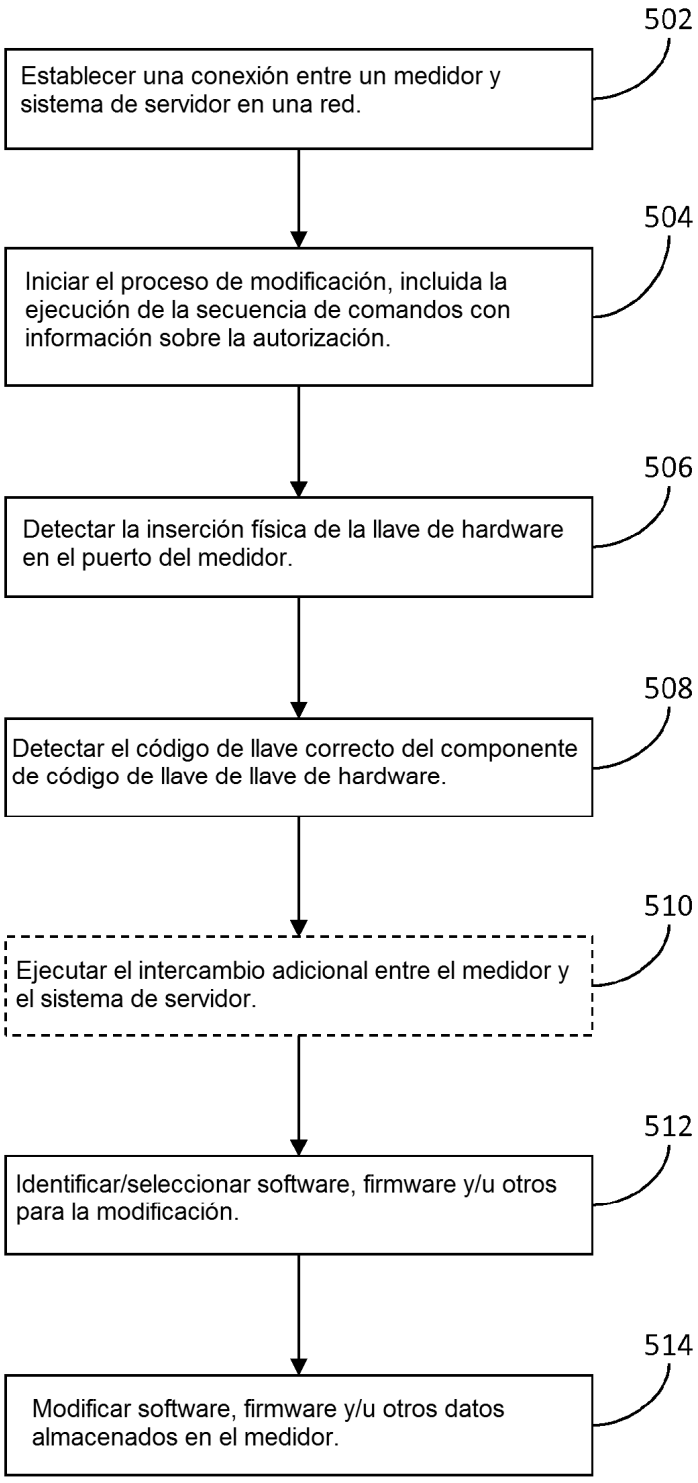
502
Establecer una conexión entre un medidor y sistema de servidor en una red.
500
504
Iniciar el proceso de modificación, incluida la ejecución de la secuencia de comandos con información sobre la autorización.
506
Detectar la inserción física de la llave de hardware en el puerto del medidor.
508
Detectar el código de llave correcto del componente de código de llave de llave de hardware.
510
Ejecutar el intercambio adicional entre el medidor y el sistema de servidor.
512
Identificar/seleccionar software, firmware y/u otros para la modificación.
514
Modificar software, firmware y/u otros datos almacenados en el medidor.

**FIG. 3**

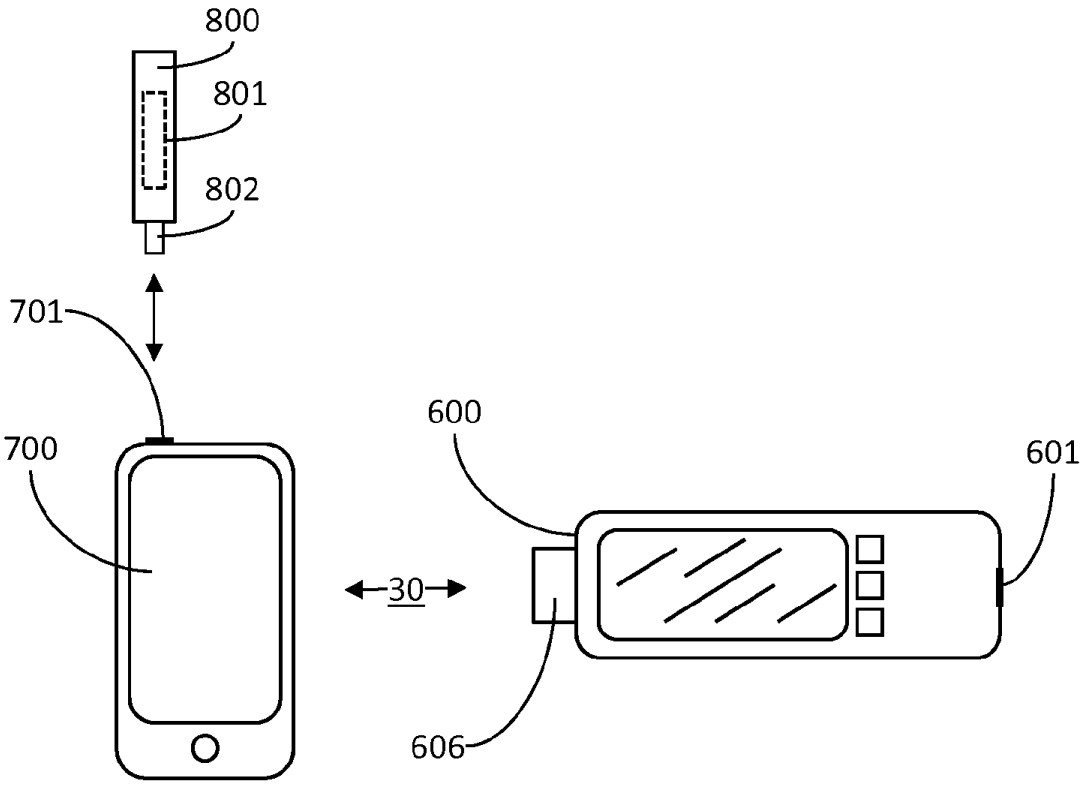
800
801
802
701
700
600
601
30
606

FIG. 4

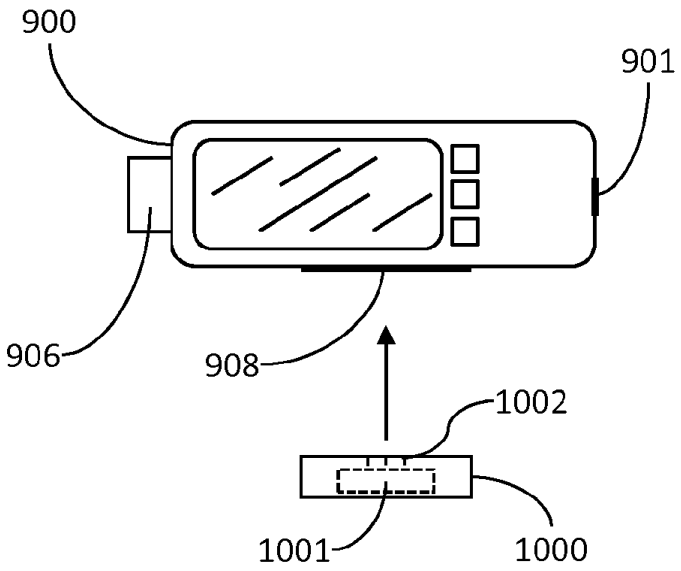
900
901
906
908
1002
1001
1000

FIG. 5