(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 745 640**

(51) Int. CI.:

G16H 40/40 (2008.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **09.08.2012 PCT/EP2012/003397**

(87) Fecha y número de publicación internacional: **14.02.2013 WO13020705**

(96) Fecha de presentación y número de la solicitud europea: **09.08.2012 E 12747977 (2)**

(97) Fecha y número de publicación de la concesión europea: **17.07.2019 EP 2742447**

(54) Título: **Distribución y revocación de datos criptográficos para dispositivos médicos portátiles**

(30) Prioridad:

11.08.2011 US 201113207934

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
03.03.2020

(73) Titular/es:

F. HOFFMANN-LA ROCHE AG (100.0%)
Grenzacherstrasse 124
4070 Basel, CH

(72) Inventor/es:

SCHWENKER, KAI-OLIVER;
TENBARGE, JAMES;
BRITWHISTLE, DANIEL;
PORSCH, ULRICH y
RACHNER, ERIC

(74) Agente/Representante:

LINAGE GONZÁLEZ, Rafael

DESCRIPCIÓN

Distribución y revocación de datos criptográficos para dispositivos médicos portátiles

CAMPO

La presente divulgación se refiere a dispositivos médicos portátiles y, más en particular, a sistemas y procedimientos de distribución y revocación de datos para dispositivos médicos portátiles.

ANTECEDENTES

La diabetes *mellitus*, a menudo denominada diabetes, es una afección crónica en la cual una persona tiene niveles de glucemia elevados que resultan de defectos en la capacidad del cuerpo para producir y/o usar insulina. Existen tres tipos principales de diabetes. La diabetes de tipo 1 normalmente afecta a niños y adultos jóvenes y puede ser autoinmunitaria, genética y/o ambiental. La diabetes de tipo 2 representa un 90-95 % de los casos de diabetes y está vinculada con la obesidad y la inactividad física. La diabetes gestacional es una forma de intolerancia a la glucosa diagnosticada durante el embarazo y normalmente desaparece espontáneamente después del parto.

En 2009, de acuerdo con la Organización Mundial de la Salud, al menos 220 millones de personas en todo el mundo padecen diabetes. En 2005, se estima que 1,1 millones de personas murieron por diabetes. La incidencia de diabetes se está incrementando rápidamente, y se estima que entre 2005 y 2030, el número de muertes por diabetes se duplicará. En los Estados Unidos, casi 24 millones de estadounidenses tienen diabetes, y se estima que un 25 por ciento de las personas mayores de 60 años están afectadas. Los Centros para el Control y Prevención de Enfermedades pronostican que 1 de cada 3 estadounidenses nacidos después del año 2000 padecerá diabetes a lo largo de su vida. El Centro Nacional de Información sobre la Diabetes (National Diabetes Information Clearinghouse) estima que la diabetes tiene un coste de 132 mil millones de $ solo en los Estados Unidos cada año. Sin tratamiento, la diabetes puede dar lugar a complicaciones graves tales como cardiopatías, apoplejías, ceguera, insuficiencia renal, amputaciones y muertes relacionadas con la neumonía y la gripe.

El control de la diabetes es complejo porque el nivel de glucemia que se incorpora al torrente sanguíneo es dinámico. La variación de la insulina en el torrente sanguíneo que controla el transporte de glucosa fuera del torrente sanguíneo también complica el control de la diabetes. Los niveles de glucemia son sensibles a la dieta y al ejercicio, pero también se pueden ver afectados por el sueño, el estrés, el tabaquismo, los viajes, las enfermedades, la menstruación y otros factores psicológicos y de estilo de vida que son exclusivos de cada paciente. La naturaleza dinámica de la glucemia y la insulina, y todos los demás factores que afectan la glucemia, a menudo requieren que una persona con diabetes pronostique los niveles de glucemia. La administración de insulina y/o medicamentos orales se puede regular y programar para mantener los niveles de glucemia dentro de un intervalo apropiado en todo momento.

El control de la diabetes a menudo es altamente molesto debido a la necesidad de obtener constantemente información de diagnóstico fiable, seguir el tratamiento prescrito y controlar el estilo de vida a diario. La información de diagnóstico, tal como el nivel de glucemia, se puede obtener a partir de una muestra de sangre capilar con un dispositivo de punción y una tira reactiva. El nivel de glucemia se mide por medio de la tira reactiva usando un glucosímetro portátil. Los niveles de glucosa intersticial se pueden obtener a partir de un sensor de glucosa en continuo que se lleva en el cuerpo.

Se puede establecer un régimen de tratamiento para un paciente en base a uno o más de los niveles de glucemia del paciente. El régimen de tratamiento puede incluir la administración de insulina y/o medicamentos orales. La insulina se puede administrar con una jeringuilla, un lápiz de insulina, una bomba de infusión ambulatoria o una combinación de dos o más de los anteriores. Con el tratamiento con insulina, determinar la cantidad de insulina que hay que inyectar en un momento dado puede requerir pronosticar la cantidad y la composición de los alimentos (por ejemplo, de grasas, carbohidratos y proteínas, y las cantidades de cada uno). Determinar la cantidad de insulina que hay que inyectar en un momento dado también puede requerir la consideración de los efectos del ejercicio y el estado fisiológico. El control de los factores de estilo de vida del paciente tales como el peso corporal, la dieta y el ejercicio puede influir significativamente en el tipo y la eficacia del tratamiento.

El control de la diabetes implica grandes cantidades de datos de diagnóstico y datos prescriptivos que se adquieren con dispositivos médicos, dispositivos de asistencia sanitaria personal, información registrada del paciente, resultados de pruebas de profesionales sanitarios, medicamentos recetados e información registrada. Los dispositivos médicos incluyen medidores automáticos de glucemia (G), monitores de glucosa en continuo, bombas de infusión de insulina, programas informáticos de análisis de diabetes y programas informáticos de configuración de dispositivos para diabetes, cada uno de los cuales genera o gestiona o ambos grandes cantidades de datos de diagnóstico y prescriptivos. Los dispositivos de asistencia sanitaria personal pueden incluir pesos, básculas, brazaletes de tensión arterial, podómetros, otros monitores de actividad y otros dispositivos adecuados. Los datos registrados del paciente pueden incluir información relacionada con los alimentos, el ejercicio y el estilo de vida. Los datos de biomarcadores de profesionales sanitarios pueden incluir HbA1C, colesterol, triglicéridos, glucosa en ayunas y tolerancia a la glucosa. La información registrada por los profesionales sanitarios puede incluir el tratamiento y otra información específica del paciente.

Con el tiempo, un dispositivo médico portátil puede quedar obsoleto. Una o más actualizaciones del programa informático ejecutadas por un dispositivo médico portátil pueden ser deseables en algunas circunstancias. Por tanto, existe una necesidad de un sistema que proporcione la capacidad de actualizar dispositivos médicos portátiles. Además, existe una necesidad de un sistema que proporcione la capacidad de actualizar los dispositivos médicos portátiles de forma segura.

La descripción de antecedentes proporcionada en el presente documento tiene el propósito de presentar en general el contexto de la divulgación. El trabajo de los autores de la invención actualmente nombrados, en la medida en que se describe en esta sección de antecedentes, así como los aspectos de la descripción que de otro modo no se pueden calificar como estado de la técnica en el momento de la presentación, no se admiten ni de manera expresa ni implícita como estado de la técnica frente a la presente divulgación.

SUMARIO

En un rasgo característico, se proporciona un procedimiento para proteger un dispositivo médico portátil de ejecutar una entidad de programa informático de ordenador instalada en la memoria del dispositivo médico portátil para su ejecución por el dispositivo médico portátil. El procedimiento incluye: recibir una lista de revocaciones desde un servidor de datos remoto en un dispositivo de configuración. La lista de revocaciones incluye N certificados criptográficos asociados con N entidades de programa informático de ordenador, respectivamente, que no se van a ejecutar por ninguno de un grupo de dispositivos médicos, incluyendo un dispositivo médico portátil. N es un número entero mayor que o igual a cero. El procedimiento incluye además recibir datos desde el dispositivo médico portátil en el dispositivo de configuración. Los datos incluyen un certificado criptográfico que está asociado con una entidad de programa informático de ordenador dada que actualmente está instalada en la memoria del dispositivo médico portátil para su ejecución por el dispositivo médico portátil. El procedimiento incluye además comparar el certificado criptográfico con la lista de revocaciones; y ejecutar selectivamente una función de protección por el dispositivo de configuración cuando el certificado criptográfico es el mismo que uno de los N certificados criptográficos de la lista de revocaciones.

En otro rasgo característico, se proporciona un procedimiento para regular la capacidad de actualización de los datos almacenados en la memoria de un dispositivo médico portátil. El procedimiento incluye: recibir una lista de revocaciones desde un primer servidor de datos remoto en un dispositivo de configuración. La lista de revocaciones incluye N certificados criptográficos asociados con N dispositivos médicos portátiles, respectivamente, a los que se les va a denegar el acceso a los datos accesibles por medio de un segundo servidor de datos remoto. N es un número entero mayor que o igual a cero. El procedimiento incluye además recibir datos desde un dispositivo médico portátil en el dispositivo de configuración. Los datos incluyen un certificado criptográfico que está asociado con el dispositivo médico portátil. El procedimiento incluye además comparar el certificado criptográfico con la lista de revocaciones; y actualizar selectivamente el dispositivo médico portátil con los datos desde el segundo servidor de datos remoto después de determinar que el certificado criptográfico no es el mismo que cualquiera de los N certificados criptográficos de la lista de revocaciones.

Otras áreas de aplicabilidad de la presente divulgación se harán evidentes a partir de la descripción detallada proporcionada a continuación en el presente documento. Se debe entender que la descripción detallada y los ejemplos específicos están previstos para el propósito de solo ilustrar y no está previsto que limiten el alcance de la divulgación.

BREVE DESCRIPCIÓN DE LOS DIBUJOS

La presente divulgación se entenderá más completamente a partir de la descripción detallada y los dibujos adjuntos, en los que:

la FIG. 1 muestra a un paciente y un profesional sanitario junto con diversos dispositivos que se pueden usar para ayudar al paciente a vigilar y controlar su salud;

la FIG. 2 muestra a un paciente con un monitor de glucosa en continuo (MGC), una bomba de infusión de insulina ambulatoria permanente, una bomba de infusión de insulina ambulatoria no permanente y un dispositivo de control de glucemia (G);

la FIG. 3 muestra un sistema de cuidado de la diabetes de sistemas que se pueden usar para controlar la diabetes;

la FIG. 4 es un diagrama de alto nivel de una implementación de ejemplo de un dispositivo de control de la diabetes portátil;

la FIG. 5 incluye un diagrama de bloques funcional de una implementación de ejemplo de un dispositivo de control de la diabetes portátil;

la FIG. 6A incluye ilustraciones de ejemplo de sistemas y procedimientos de comunicación seguros;

la FIG. 6B incluye un diagrama de bloques funcional de un sistema de distribución de datos de ejemplo; y

la FIG. 7 incluye una ilustración de ejemplo de un procedimiento para controlar la distribución de datos a un dispositivo médico portátil.

DESCRIPCIÓN DETALLADA

La siguiente descripción es de naturaleza meramente ilustrativa y de ninguna manera pretende limitar la divulgación, su aplicación o usos. Para propósitos de claridad, se usarán los mismos números de referencia en los dibujos para identificar elementos similares. Como se usa en el presente documento, la frase "al menos uno de A, B y C" se debe interpretar como una lógica (A o B o C), usando una lógica no exclusiva o. Se debe entender que las etapas dentro de un procedimiento se pueden ejecutar en un orden diferente sin alterar los principios de la presente divulgación.

En referencia ahora a la FIG. 1, un paciente 100 con diabetes y un profesional sanitario 102 se muestran en un entorno clínico. Al paciente 100 con diabetes se le puede diagnosticar un síndrome metabólico, prediabetes, diabetes de tipo 1, diabetes de tipo 2, diabetes gestacional, etc. El personal sanitario para la diabetes es diverso e incluye enfermeras, enfermeras facultativas, médicos, endocrinólogos y otros y se denominan conjuntamente profesionales sanitarios.

Durante una consulta sanitaria, el paciente 100 típicamente comparte con el profesional sanitario 102 una variedad de datos que incluyen mediciones de glucemia (G), datos del monitor de glucosa en continuo, cantidades y tipo de insulina administrada, cantidades de alimentos y bebidas consumidas, horarios de ejercicio, estado de salud y otra información de estilo de vida. El profesional sanitario 102 puede obtener datos adicionales para el paciente 100, tales como mediciones de HbA1C, niveles de colesterol, glucosa en plasma, triglicéridos, tensión arterial y peso. Los datos se pueden registrar de forma manual o electrónica en un dispositivo de control de la diabetes portátil 104 (por ejemplo, un dispositivo de vigilancia de G portátil), un programa informático de análisis de la diabetes ejecutado en un ordenador personal (PC) 106 y/o un sitio web de análisis de la diabetes. El profesional sanitario 102 puede analizar los datos del paciente de forma manual o electrónica usando el programa informático de análisis de la diabetes y/o el sitio web de análisis de la diabetes. Después de analizar los datos y revisar cómo de eficaz es el tratamiento prescrito previamente y cómo de bien sigue el paciente 100 el tratamiento prescrito previamente, el profesional sanitario 102 puede decidir si modifica un tratamiento prescrito para el paciente 100.

En referencia ahora a la FIG. 2, el paciente 100 puede usar un monitor de glucosa en continuo (MGC) 200, una bomba de infusión de insulina ambulatoria permanente 204 o una bomba de infusión de insulina ambulatoria no permanente 202 (conjuntamente, bomba de insulina 204), y el dispositivo de control de la diabetes 104. El MGC 200 puede usar un sensor subcutáneo para detectar y vigilar la cantidad de glucosa (por ejemplo, la concentración de glucosa) del paciente 100. El MGC 200 comunica las mediciones de glucosa al dispositivo de control de la diabetes 104.

El dispositivo de control de la diabetes 104 realiza diversas tareas incluyendo medir y registrar mediciones de G, determinar una cantidad de insulina que se va a administrar al paciente 100 por medio de la bomba de insulina 204, recibir una entrada del usuario por medio de una interfaz de usuario, archivar datos, realizar pruebas estructuradas de G, etc. El dispositivo de control de la diabetes 104 puede transmitir instrucciones a la bomba de insulina 204, y la bomba de insulina 204 administra insulina selectivamente al paciente 100. La insulina se puede administrar en forma de una dosis de inyección intravenosa rápida prandial, una dosis de inyección intravenosa rápida de corrección, una dosis basal, etc.

En referencia ahora a la FIG. 3, se muestra un sistema de control de la diabetes 300 que se puede usar por el paciente 100 y/o el profesional sanitario 102. El sistema 300 puede incluir uno o más de los siguientes dispositivos: el dispositivo de control de la diabetes 104, el MGC 200, la bomba de insulina 204, un dispositivo móvil 302, el programa informático de control de la diabetes ejecutado en el ordenador 106 y uno o más de otros dispositivos sanitarios 304. El dispositivo de control de la diabetes 104 se puede configurar como un "nodo" del sistema y comunicarse con uno o más de los otros dispositivos del sistema 300. La bomba de insulina 204, el dispositivo móvil 302 u otro dispositivo adecuado pueden servir de forma alternativa como nodo del sistema. La comunicación entre diversos dispositivos en el sistema 300 se puede realizar usando interfaces inalámbricas (por ejemplo, Bluetooth) y/o interfaces cableadas (por ejemplo, USB). Los protocolos de comunicación usados por estos dispositivos pueden incluir protocolos que cumplan con la norma IEEE 11073 como se extienden usando las pautas proporcionadas por las Directrices de diseño de Continua Health Alliance. Además, se pueden usar los sistemas de registros sanitarios tales como Microsoft HealthVault™ y Google Health™ por el paciente 100 y el profesional sanitario 102 para intercambiar información.

El programa informático de control de la diabetes que se ejecuta en el ordenador 106 puede incluir un analizador-configurador que almacena información de configuración para los dispositivos del sistema 300. Solo como ejemplo, el configurador tiene una base de datos para almacenar información de configuración para el dispositivo de control de la diabetes 104 y los otros dispositivos. Un paciente puede interactuar con el configurador a través de interfaces de usuario gráficas (GUI) estándar de ordenador o basadas en la web. El configurador transmite selectivamente configuraciones aprobadas por el paciente a los dispositivos del sistema 300. El analizador recupera selectivamente datos desde los dispositivos del sistema 300, almacena los datos en una base de datos, analiza selectivamente los datos y genera los resultados de análisis a través de GUI estándar de ordenador o basadas en la web.

En referencia ahora a la FIG. 4, se presenta una ilustración de alto nivel de un modo de realización de ejemplo del dispositivo de control de la diabetes 104. El dispositivo de control de la diabetes 104 incluye, entre otras cosas, una

carcasa 404, interruptores de control de la unidad de usuario (no específicamente numerados), una pantalla táctil 408 y un puerto para tiras reactivas de G 420. Los interruptores de control de la unidad de usuario, por ejemplo, pueden incluir interruptores de ENCENDIDO/APAGADO, interruptores de volumen, interruptores de alarma para pruebas de G y/o administración de insulina, y/o uno o más de otros interruptores u otros tipos de dispositivos de control que un paciente puede usar para controlar funciones/operaciones del dispositivo de control de la diabetes 104.

Se puede insertar una tira reactiva de G 416 en el puerto para tiras reactivas de G 420. La tira reactiva de G 416 se puede insertar en el puerto para tiras reactivas de G 420 por un paciente, desde un cartucho de tiras reactivas (no mostrado) localizado dentro de la carcasa 404, o de otra manera adecuada. La tira reactiva de G 416 se muestra ya insertada en el puerto para tiras reactivas de G 420 en el ejemplo de la FIG. 4 y aún no insertada en el puerto para tiras reactivas de G 420 en el ejemplo de la FIG. 5.

Las opciones seleccionables por el usuario 424 se pueden presentar en una parte de la pantalla 408. Las opciones seleccionables 424 pueden incluir una opción de menú 428, una opción de insulina de inyección intravenosa rápida 432, una opción de carbohidratos 436 y una opción de acontecimiento 440. Una o más de otras opciones seleccionables por el usuario pueden estar disponibles adicionalmente o de forma alternativa. El paciente puede acceder al menú de un dispositivo para el dispositivo de control de la diabetes 104 seleccionando la opción de menú 428. El paciente puede introducir diversa información de insulina (y/u otro medicamento) (por ejemplo, cantidad, tipo de insulina, etc.) seleccionando la opción de insulina de inyección intravenosa rápida 432. El paciente puede introducir diversa información sobre la ingesta de carbohidratos (por ejemplo, la cantidad) seleccionando la opción de carbohidratos 436. El paciente también puede introducir otra información de ingesta de alimentos (por ejemplo, contenido de proteínas, contenido de grasa, etc.) seleccionando la opción de carbohidratos 436. El paciente puede introducir diversa información relacionada con acontecimientos (por ejemplo, alimentos, ejercicio, períodos de estrés, etc.) que pueden afectar a las mediciones de G del paciente seleccionando la opción de acontecimiento 440.

Aunque la pantalla 408 se describe en el presente documento como una pantalla táctil, el dispositivo de control de la diabetes 104 puede incluir otra forma adecuada de pantalla (por ejemplo, LED, etc.). Si no se usa una pantalla táctil, los interruptores de control del usuario pueden incluir botones o controles específicos mediante los cuales el paciente puede seleccionar diversas opciones y marcadores de entrada necesarios para hacer funcionar el dispositivo de control de la diabetes 104.

La descripción anterior es una descripción general del dispositivo de control de la diabetes 104. En la práctica, el dispositivo de control de la diabetes 104 puede incluir controles adicionales, puertos de entrada, puertos de salida, etc., como se puede desear para potenciar adicionalmente su utilidad o su uso con otros componentes y dispositivos (por ejemplo, ordenadores, bombas de infusión, teléfonos móviles, etc.). La descripción del dispositivo de control de la diabetes 104 no se debe tomar como limitante en cuanto a la construcción del dispositivo de control de la diabetes 104 o en cuanto a los rasgos característicos y capacidades del dispositivo de control de la diabetes 104.

Como se usa en el presente documento, el término "módulo" se puede referir, formar parte de, o incluir un circuito integrado específico de la aplicación (ASIC); un circuito electrónico; un circuito de lógica combinacional; una matriz de puertas programables *in situ* (FPGA); un procesador (compartido, dedicado o grupal) que ejecuta código; otros componentes adecuados que proporcionan la funcionalidad descrita; o una combinación de algunos o todos los anteriores, tal como en un sistema en chip. El término "módulo" puede incluir memoria (compartida, dedicada o grupal) que almacena código ejecutado por el procesador.

El término "código", como se usa anteriormente, puede incluir programa informático, *firmware* y/o microcódigo, y se puede referir a programas, rutinas, funciones, clases y/u objetos. El término "compartido", como se usa anteriormente, significa que parte o todo el código de múltiples módulos se puede ejecutar usando un único procesador (compartido). Además, parte o todo el código de múltiples módulos se puede almacenar por una única memoria (compartida). El término "grupal", como se usa anteriormente, significa que parte o todo el código de un único módulo se puede ejecutar usando un grupo de procesadores. Además, parte o todo el código de un único módulo se pueden almacenar usando un grupo de memorias.

Los aparatos y procedimientos descritos en el presente documento se pueden implementar por uno o más programas de ordenador ejecutados por uno o más procesadores. Los programas de ordenador incluyen instrucciones ejecutables por procesador que se almacenan en un medio legible por ordenador, tangible, no transitorio. Los programas de ordenador también pueden incluir datos almacenados. Los ejemplos de medios legibles por ordenador, tangibles, no transitorios incluyen, pero no se limitan a, memoria no volátil, almacenamiento magnético y almacenamiento óptico.

En referencia ahora a la FIG. 5, se presenta un diagrama de bloques funcional del dispositivo de control de la diabetes 104. Si bien la presente divulgación se analizará junto con el dispositivo de control de la diabetes 104, la presente divulgación también es aplicable a otros dispositivos médicos portátiles, incluyendo bombas de insulina, MGC y otros tipos de dispositivos médicos portátiles.

El dispositivo de control de la diabetes 104 puede incluir un módulo procesador (por ejemplo, un subsistema basado en microprocesador) 504 que puede recibir información desde un motor de medición de G 508. El motor de medición de G 508 se puede localizar adyacente al puerto para tiras reactivas de G 420. El motor de medición de G 508 lee (mide) un

nivel de G de la tira reactiva de G 416 insertada en el puerto para tiras reactivas de G 420. El motor de medición de G 508 puede incluir un módulo de clave de código 512 que incluye datos precalibrados para determinar un nivel de G a partir de la tira reactiva de G 416. La tira reactiva de G 416 se puede proporcionar de las tiras reactivas de G sin usar del cartucho de tiras reactivas de la carcasa dentro del dispositivo de control de la diabetes 104.

El motor de medición de G 508 genera datos de muestras de G 516 en base a su lectura de la tira reactiva de G 416. Entre otras cosas, los datos de muestras de G 516 incluyen datos indicativos del nivel de G de una muestra de sangre en la tira reactiva de G 416. El módulo procesador 504 también puede recibir datos de muestras de G de otras fuentes, tales como por medio del MGC 200, la pantalla 408 y/u otra fuente adecuada. El módulo procesador 504 puede recibir datos de entrada del usuario por medio de uno o más dispositivos de entrada/salida (E/S) del usuario 514, tales como la pantalla 408, uno o más botones/interruptores/etc., y/o uno o más de otros dispositivos de E/S del usuario.

El motor de medición de G 508 también puede generar los datos de muestras de G 516 para indicar la fecha y la hora en que se leyó la tira reactiva de G 416. En otras palabras, el motor de medición de G 508 puede incluir una marca de tiempo con los datos de muestra de G 516. En diversas implementaciones, el módulo procesador 504 puede selectivamente crear una marca de tiempo de los datos de muestras de G 516 y puede crear una marca de tiempo de los datos de entrada del usuario y otros datos cuando se reciben.

Un reloj 518 puede proporcionar la fecha y la hora. El paciente puede configurar la fecha y hora actuales, y el reloj 518 después de esto realiza un seguimiento de la fecha y hora actuales. En diversas implementaciones, la fecha y hora actuales se pueden adquirir desde (por ejemplo, sincronizarse con) el ordenador 106.

El dispositivo de control de la diabetes 104 incluye un almacén de datos 532. Solo como ejemplo, el almacén de datos 532 puede incluir una memoria y/o uno o más de otros medios legibles por ordenador, tangibles, adecuados. Se pueden almacenar diversos datos en el almacén de datos 532. Solo como ejemplo, una entidad de programa informático de ordenador 536 se almacena en el almacén de datos 532. La entidad de programa informático de ordenador 536 puede incluir, por ejemplo, firmware, programa informático, variables, etc. El módulo procesador 504 ejecuta selectivamente partes de la entidad de programa informático de ordenador 536 para realizar las funciones del dispositivo de control de la diabetes 104.

La entidad de programa informático de ordenador 536 se puede escribir en el almacén de datos 532 antes de que el dispositivo de control de la diabetes 104 se comercialice. La entidad de programa informático de ordenador 536 se puede actualizar después de que se comercialice el dispositivo de control de la diabetes 104. La entidad de programa informático de ordenador 536 se puede actualizar, por ejemplo, por medio del programa informático que se ejecuta en el ordenador 106 o por medio de un servidor de datos remoto (véase también la FIG. 6B).

Los datos del dispositivo 540 también se pueden almacenar en el almacén de datos 532. Los datos del dispositivo 540 pueden incluir, por ejemplo, datos del tipo de producto, datos de la versión del producto, datos de la región, un certificado de programa informático, un identificador de dispositivo exclusivo, un certificado de dispositivo/usuario y otros datos específicos del dispositivo adecuados. Los datos del tipo de producto pueden indicar, por ejemplo, el dispositivo de control de G, la bomba de insulina, el MGC, etc. Los datos de la versión del producto pueden indicar, por ejemplo, una versión (o generación) del dispositivo de control de la diabetes 104, un nombre/número de modelo, etc. El certificado de programa informático puede incluir, por ejemplo, una versión o identificador de la entidad de programa informático de ordenador 536 y otros datos adecuados. El certificado de programa informático es un certificado criptográfico (digital). El certificado de programa informático también se puede denominar un certificado de código. El identificador del dispositivo exclusivo puede incluir datos que son exclusivos para el dispositivo de control de la diabetes 104, tal como un número de serie u otro identificador exclusivo adecuado. El certificado de dispositivo/usuario es un certificado criptográfico (digital) que es exclusivo para el dispositivo de control de la diabetes 104.

Los datos criptográficos 544 también se pueden almacenar en el almacén de datos 532. Los datos criptográficos 544 se pueden usar, por ejemplo, para cifrar mensajes transmitidos por el dispositivo de control de la diabetes 104 a otro dispositivo, descifrar los mensajes recibidos por el dispositivo de control de la diabetes 104 desde otro dispositivo, autenticar, verificar y otras funciones criptográficas. Solo como ejemplo, los datos criptográficos 544 pueden incluir una o más claves (por ejemplo, públicas), uno o más algoritmos de cifrado, uno o más algoritmos de descifrado y otros datos criptográficos adecuados.

En referencia ahora a la FIG. 6A, se presentan implementaciones de ejemplo de un sistema de comunicación segura 600 y un procedimiento de comunicación segura 602. El sistema de comunicación segura 600 incluye un gestor 604 y un agente 606. El gestor 604 se puede comunicar con uno o más de otros agentes, y el agente 606 se puede comunicar con uno o más de otros gestores. Se analizará la comunicación entre el gestor 604 y el agente 606, pero el siguiente análisis es aplicable a la comunicación entre otros gestores y agentes.

El gestor 604 y el agente 606 se pueden comunicar, por ejemplo, junto con el gestor 604 actualizando los datos almacenados en la memoria del agente 606. Sin embargo, la comunicación entre el gestor 604 y el agente 606 se realiza de acuerdo con un protocolo para garantizar que la comunicación sea segura. El protocolo se puede ajustar a la norma de criptografía RSA de acuerdo con el volumen n.º 1 de las normas de criptografía de clave pública (PKCS) de RSA

Laboratories u otro protocolo criptográfico adecuado. El protocolo puede implicar el uso de un algoritmo hash criptográfico SHA-2 (por ejemplo, SHA-256), un algoritmo hash criptográfico SHA-3 u otro algoritmo hash criptográfico adecuado.

A cada gestor se le puede atribuir una de una pluralidad de funciones diferentes. Un gestor que da servicio como una función puede ser capaz de actualizar tipos de datos predeterminados almacenados en la memoria del agente 606. Cada función diferente se puede asociar con la capacidad de actualizar diferentes tipos de datos predeterminados. La capacidad de actualizar diferentes tipos de datos se puede basar en el principio de privilegio mínimo. Más específicamente, un gestor que da servicio según una primera función puede ser capaz de actualizar un primer conjunto de tipos de datos almacenados en la memoria del agente 606. Un gestor que da servicio según una segunda función puede ser capaz de actualizar el primer conjunto de tipos de datos y, además, ser capaz de actualizar un segundo conjunto de tipos de datos almacenados en la memoria del agente 606. Un gestor que da servicio según una tercera función puede ser capaz de actualizar un tercer conjunto de tipos de datos además del primer y segundo conjuntos de tipos y así sucesivamente. Los agentes se pueden configurar para aceptar actualizaciones solo de los gestores que den servicio según una o más de la pluralidad de funciones.

El gestor 604 tiene una clave criptográfica pública. El gestor 604 también tiene una clave criptográfica privada. La clave criptográfica privada también incluye datos con respecto a la clave criptográfica pública. El gestor 604 firma criptográficamente los mensajes que transmite al agente 606 usando la clave privada y un algoritmo de cifrado. El agente 606 usa la clave pública y un algoritmo de descifrado para verificar que el mensaje firmado se envió por una fuente de confianza (por ejemplo, el gestor 604) y que el mensaje firmado no se modificó antes de su recepción por el agente 606. El procedimiento de firmar un mensaje y verificar que el mensaje firmado se envió por una fuente de confianza se puede realizar como parte de un procedimiento de autenticación. El gestor 604 y el agente 606 pueden realizar la autenticación para garantizar que la comunicación entre el gestor 604 y el agente 606 sea segura antes de que el gestor 604 pueda actualizar los datos almacenados en la memoria del agente 606.

Un ejemplo de autenticación se ilustra en 602. El gestor 604 puede transmitir una solicitud de autenticación 610 al agente 606 para iniciar la autenticación de comunicación segura entre el gestor 604 y el agente 606. La solicitud de autenticación 610 puede incluir, por ejemplo, la función del gestor 604, la clave pública y/u otros datos adecuados. En diversas implementaciones, la solicitud de autenticación 610 puede tener la forma de un certificado digital.

El agente 606 puede determinar si el agente 606 se configura para aceptar actualizaciones desde la función del gestor 604. Si no, el agente 606 puede transmitir un código de error predeterminado al gestor 604 y finalizar la autenticación. Si es así, el agente 606 puede generar un desafío de autenticación 612 y transmitir el desafío de autenticación 612 al gestor 604. El agente 606 genera el desafío de autenticación 612 de forma aleatoria. Solo como ejemplo, el agente 606 puede generar el desafío de autenticación 612 de forma aleatoria usando un generador de números aleatorios, tal como un generador de números aleatorios que cumple con la Publicación Especial 800-90 del NIST, titulada "Recomendación para la generación de números aleatorios usando generadores de bits aleatorios deterministas" (marzo de 2007).

El gestor 604 firma digitalmente el desafío de autenticación 612 usando la clave privada y transmite el desafío de autenticación firmado al agente 606 en forma de una respuesta de desafío 614. En base a la clave pública y al desafío de autenticación 612, el agente 606 determina si la respuesta de desafío 614 es auténtica. En otras palabras, el agente 606 verifica la firma usando la clave pública y el desafío de autenticación 612. El agente 606 notifica al gestor 604 si la autenticación ha sido satisfactoria o fallida por medio de un resultado de autenticación 616.

Si la autenticación ha sido satisfactoria, el gestor 604 puede actualizar selectivamente los datos almacenados en la memoria del agente 606. La autenticación también se puede realizar entre el gestor 604 y un servidor (por ejemplo, la FIG. 6B) para garantizar una comunicación segura entre el gestor 604 y el servidor. Antes de que el gestor 604 cree o modifique un archivo que se va a cargar en el agente 606, el gestor 604 firma el archivo usando la clave privada asociada con su función. El gestor 604 puede firmar el archivo usando la clave privada, RSA y el algoritmo SHA-2. El resultado de la firma es un hash firmado de los datos que se firman. La clave privada asociada con una o más de las funciones puede no ser elegible para usar para firmar un archivo.

Cuando el agente 606 recibe un archivo desde el gestor 604, el agente 606 verifica la firma digital proporcionada con el archivo. El gestor 604 puede notificar al agente 606 qué clave pública usar para verificar la firma. El agente 606 puede verificar el archivo (u otros datos firmados entrantes, tales como la respuesta de desafío 614) llamando a una interfaz de programación de aplicaciones (API) usada para la verificación. El agente 606 puede proporcionar la clave pública, el archivo firmado y los datos originales para la API. Los algoritmos que va a usar la API también se pueden especificar, y los algoritmos pueden ser, por ejemplo, RSA y el algoritmo SHA-2. El agente 606 puede evitar usar los datos transmitidos si la verificación ha sido fallida.

En referencia ahora a la FIG. 6B, se presenta un diagrama de bloques funcional de un sistema de distribución de datos de ejemplo. Los ejemplos del agente 606 pueden ser el dispositivo de control de la diabetes 104, la bomba de insulina 204, el MGC 200, el dispositivo móvil 304 y otros dispositivos médicos portátiles. Un ejemplo del gestor 604 puede ser un dispositivo de configuración 650. Solo como ejemplo, el dispositivo de configuración 650 puede incluir una aplicación (por ejemplo, programa informático) ejecutada en un ordenador, tal como el ordenador 106. La entidad de programa informático de ordenador 536 almacenada en el almacén de datos 532 del dispositivo de control de la diabetes 104 se

puede actualizar. La entidad de programa informático de ordenador 536 se puede actualizar en respuesta a una solicitud de entrada del usuario para actualizar la entidad de programa informático de ordenador 536 cuando el dispositivo de control de la diabetes 104 se conecta al dispositivo de configuración 650. Un usuario puede introducir una solicitud de este tipo al dispositivo de configuración 650 o al dispositivo de control de la diabetes 104. En diversas implementaciones, la entidad de programa informático de ordenador 536 se puede actualizar automáticamente cuando el dispositivo de control de la diabetes 104 y el dispositivo de configuración 650 se conectan. La conexión puede ser cableada o inalámbrica.

Para actualizar la entidad de programa informático de ordenador 536, el dispositivo de configuración 650 puede reemplazar una o más partes de la entidad de programa informático de ordenador 536 o reemplazar la entidad de programa informático de ordenador 536 con otra entidad de programa informático de ordenador. El dispositivo de configuración 650 actualiza la entidad de programa informático de ordenador 536 con datos descargados desde un servidor de distribución de datos 654.

Antes de actualizar la entidad de programa informático de ordenador 536, el dispositivo de configuración 650 puede obtener el certificado de dispositivo/usuario del dispositivo de control de la diabetes 104. El dispositivo de configuración 650 puede verificar que el dispositivo de control de la diabetes 104 está registrado y autorizado para actualizarse. En diversas implementaciones, la autenticación/verificación se puede realizar por medio de la comunicación entre el dispositivo de configuración 650 y un servidor de autenticación 658. El servidor de autenticación 658 puede ser diferente del servidor de distribución de datos 654.

El certificado de dispositivo/usuario puede incluir un vencimiento. Si el certificado de dispositivo/usuario ha caducado previamente, es posible que el dispositivo de configuración 650 no permita que se actualice la entidad del programa informático de ordenador 536. El dispositivo de configuración 650 también puede recibir una primera lista de revocaciones de certificados (LRC) desde el servidor de autenticación 658. Una LRC también se puede denominar una lista de revocaciones.

La primera LRC puede incluir una lista de certificados de dispositivo/usuario no caducados que no son elegibles para recibir datos por medio del servidor de distribución de datos 654. La primera LRC también puede incluir certificados de dispositivo/usuario caducados que no son elegibles para recibir datos por medio del servidor de distribución de datos 654. Si el certificado de dispositivo/usuario del dispositivo de control de la diabetes 104 está en la primera LRC (por ejemplo, la misma que uno de los certificados de dispositivo/usuario en la primera LRC), es posible que el dispositivo de configuración 650 no permita que se actualice la entidad de programa informático de ordenador 536. Si el certificado de dispositivo/usuario no está en la primera LRC, el dispositivo de configuración 650 puede actualizar el dispositivo de control de la diabetes 104 en base a los datos del servidor de distribución de datos 654.

El dispositivo de configuración 650 también puede realizar una o más acciones cuando el certificado de dispositivo/usuario del dispositivo de control de la diabetes 104 está en la primera LRC. Solo como ejemplo, el dispositivo de configuración 650 puede intentar obtener un nuevo certificado de dispositivo/usuario (no caducado) para el dispositivo de control de la diabetes 104, presentar una indicación de que el dispositivo de control de la diabetes 104 no es elegible para su actualización (por ejemplo, por medio de una pantalla del dispositivo de configuración 650 y/o una pantalla del dispositivo de control de la diabetes 104) y/o realizar una o más acciones adecuadas.

Los datos para actualizar dispositivos médicos portátiles autorizados y registrados, incluyendo el dispositivo de control de la diabetes 104, se pueden almacenar en una base de datos 672. A la base de datos 672 puede acceder el servidor de distribución de datos 654. Los datos específicos del dispositivo para cada dispositivo médico portátil autorizado y registrado también se pueden almacenar en la base de datos 672. Solo como ejemplo, cada vez que se actualiza el dispositivo de control de la diabetes 104, los datos para el dispositivo de control de la diabetes 104 almacenados en la base de datos 672 se actualizan de modo que la base de datos 672 incluye datos indicativos de las últimas características conocidas de cada dispositivo médico portátil.

El dispositivo de configuración 650 puede obtener selectivamente datos de programa informático del servidor de distribución de datos 654 para el dispositivo de control de la diabetes 104. Los datos de programa informático del servidor de distribución de datos 654 indican que una entidad de programa informático de ordenador actual de la que la base de datos 672 tiene un registro se está instalando y ejecutando por el dispositivo de control de la diabetes 104. El dispositivo de configuración 650 también puede obtener el certificado de programa informático del dispositivo de control de la diabetes 104. El dispositivo de configuración 650 puede comparar los datos de versión obtenidos del servidor de distribución de datos 654 con los datos de versión indicados en el certificado de programa informático obtenido del dispositivo de control de la diabetes 104. El dispositivo de configuración 650 puede notificar al servidor de distribución de datos 654 si los dos difieren. Si los datos de la versión son diferentes, el dispositivo de configuración 650 puede realizar una o más acciones de protección. Las acciones de protección de ejemplo se analizan más adelante.

El dispositivo de configuración 650 también puede obtener una segunda LRC del servidor de distribución de datos 654. La segunda LRC puede incluir una lista de entidades de programa informático de ordenador que no se van a ejecutar por ninguno de un grupo de dispositivos médicos portátiles, incluyendo el dispositivo de control de la diabetes 104. El dispositivo de configuración 650 puede determinar si el certificado de programa informático para la entidad de programa informático de ordenador 536 está en la segunda LRC.

Si el certificado de programa informático para la entidad de programa informático de ordenador 536 está en la segunda LRC, el dispositivo de configuración 650 puede realizar una o más acciones de protección. Solo como ejemplo, el dispositivo de configuración 650 puede evitar que el módulo procesador 504 ejecute la entidad de programa informático de ordenador 536 en el futuro. El dispositivo de configuración 650 puede evitar que el módulo procesador 504 ejecute la entidad de programa informático de ordenador 536, por ejemplo, cambiando el estado de una bandera u otro indicador que el módulo procesador 504 comprueba antes de ejecutar cualquier parte de la entidad de programa informático de ordenador 536. Solo como otro ejemplo, el dispositivo de configuración 650 puede presentar un mensaje predeterminado en la pantalla del dispositivo de control de la diabetes 104 y/o el dispositivo de configuración 650. Solo como otro ejemplo más, el dispositivo de configuración 650 puede pedir a un usuario que introduzca un acuse de recibo. Solo como otro ejemplo, el dispositivo de configuración 650 puede actualizar la entidad de programa informático de ordenador 536 en base a otra entidad de programa informático de ordenador asociada con un certificado de programa informático que no está en la segunda LRC.

El dispositivo de configuración 650 puede recibir datos que indiquen posibles actualizaciones que están disponibles para el dispositivo de control de la diabetes 104. El dispositivo de configuración 650 puede presentar las posibles actualizaciones para su selección por un usuario. El dispositivo de configuración 650 puede presentar las posibles actualizaciones por medio de la pantalla del dispositivo de control de la diabetes 104 y/o la pantalla del ordenador 106.

Un usuario puede seleccionar una o más de las posibles actualizaciones. El dispositivo de configuración 650 puede actualizar los datos almacenados en el almacén de datos 532 del dispositivo de control de la diabetes 104 en base a las posibles actualizaciones seleccionadas. Solo como ejemplo, el dispositivo de configuración 650 puede actualizar la entidad de programa informático de ordenador 536 en base a una entidad de programa informático de ordenador seleccionada. El dispositivo de configuración 650 también puede realizar una autenticación para verificar que el usuario es elegible para actualizar el dispositivo de control de la diabetes 104. El dispositivo de configuración 650 se puede abstener de actualizar el dispositivo de control de la diabetes 104 si el usuario no es elegible para actualizar el dispositivo de control de la diabetes 104. Después de una actualización, el módulo procesador 504 ejecuta la entidad de programa informático de ordenador seleccionada para controlar la funcionalidad del dispositivo de control de la diabetes 104. El dispositivo de configuración 650 puede actualizar los datos del dispositivo 540, los datos de criptografía 544 y/u otros datos adecuados para reflejar la actualización.

Después de actualizar el dispositivo de control de la diabetes 104, el dispositivo de configuración 650 solicita al servidor de distribución de datos 654 actualizar los datos almacenados en la base de datos 672 para que el dispositivo de control de la diabetes 104 refleje la actualización del dispositivo de control de la diabetes 104. De esta manera, los datos almacenados en la base de datos 672 para el dispositivo de control de la diabetes 104 reflejan el estado actual de la entidad de programa informático de ordenador 536 instalada en el dispositivo de control de la diabetes 104 para su ejecución por el dispositivo de control de la diabetes 104.

En referencia ahora a la FIG. 7, se presenta un procedimiento de ejemplo de regulación de la distribución de datos para dispositivos médicos portátiles. El dispositivo de configuración 650 puede consultar 704 el dispositivo de control de la diabetes 104 para obtener los datos del dispositivo almacenados en el almacén de datos 532 del dispositivo de control de la diabetes 104. Solo como ejemplo, el dispositivo de configuración 650 puede consultar el dispositivo de control de la diabetes 104 para obtener el certificado de dispositivo/usuario y el certificado de programa informático del dispositivo de control de la diabetes 104. El dispositivo de configuración 650 puede generar la consulta 704 en respuesta a una solicitud de actualización (no mostrada), automáticamente en un momento en que el dispositivo de control de la diabetes 104 está conectado al dispositivo de configuración 650, o en otro momento adecuado. El dispositivo de control de la diabetes 104 transmite los datos del dispositivo 708 al dispositivo de configuración 650 en respuesta a la consulta 704.

El dispositivo de configuración 650 puede transmitir una solicitud de autenticación 712 al servidor de autenticación 658. El dispositivo de configuración 650 puede transmitir la solicitud de autenticación 712, por ejemplo, junto con la autenticación del certificado de dispositivo/usuario y la verificación de que el dispositivo de control de la diabetes 104 es elegible para recibir actualizaciones desde el servidor de distribución de datos 654. El dispositivo de configuración 650 puede transmitir la solicitud de autenticación 712 u otra solicitud de autenticación, por ejemplo, junto con la autenticación de un usuario del dispositivo de configuración 650 y la verificación de que el usuario es elegible para actualizar el dispositivo de control de la diabetes 104 y/o el tipo de datos que se van a actualizar. El servidor de autenticación 658 puede transmitir una respuesta de autenticación 716 en base al resultado de la autenticación y verificación. En diversas implementaciones, el servidor de autenticación 658 puede transmitir los datos necesarios al dispositivo de configuración 650 para que el dispositivo de configuración 650 realice la autenticación y verificación, o los datos necesarios se pueden almacenar previamente en la memoria del dispositivo de configuración 650. La respuesta de autenticación 716 puede indicar si la autenticación y la verificación han sido satisfactorias o fallidas.

El servidor de autenticación 658 también puede transmitir la primera LRC 720 al dispositivo de configuración 650 en respuesta a la solicitud de autenticación 712. El dispositivo de configuración 650 compara el certificado de dispositivo/usuario con la primera LRC 720. Si el certificado de dispositivo/usuario está en la primera LRC 720, el dispositivo de configuración 650 puede tomar una o más acciones de certificado revocado 724.

Si el certificado de dispositivo/usuario no está en la primera LRC 720, el dispositivo de configuración 650 puede transmitir una consulta de información más reciente 728 al servidor de distribución de datos 654. La consulta de información más reciente 728 puede solicitar los datos más recientes que se almacenan en la base de datos 672 para el dispositivo de control de la diabetes 104. Más específicamente, la consulta de información más reciente 728 puede solicitar la información más reciente que se almacena en la base de datos 672 con respecto a una entidad de programa informático de ordenador almacenada en el almacén de datos 532 del dispositivo de control de la diabetes 104.

El servidor de distribución de datos 654 recupera la información del dispositivo más reciente 732 en respuesta a la solicitud y transmite la información del dispositivo más reciente 732 al dispositivo de configuración 650. El servidor de distribución de datos 654 también transmite la segunda LRC 736 al dispositivo de configuración 650. El dispositivo de configuración 650 puede transmitir una notificación (no mostrada) al servidor de distribución de datos 654 si la entidad de programa informático de ordenador 536 almacenada en el almacén de datos 532 es diferente de la entidad de programa informático de ordenador indicada por medio de la información del dispositivo más reciente 732.

El dispositivo de configuración 650 compara el certificado de programa informático almacenado en el almacén de datos 532 del dispositivo de control de la diabetes 104 con la segunda LRC 736. Si el certificado de programa informático está en la segunda LRC 736, el dispositivo de configuración 650 puede tomar una o más acciones de protección 740, tales como actualizar la entidad de programa informático de ordenador 536 en base a otra entidad de programa informático de ordenador. Una vez completado, el dispositivo de control de la diabetes 104 puede transmitir un resultado 744 de la una o más acciones de protección 740 al dispositivo de configuración 650. El dispositivo de configuración 650 puede transmitir una actualización de resultados 748 al servidor de distribución de datos 654. La actualización de resultados 748 puede indicar el resultado 744 de la una o más acciones de protección 740. El servidor de distribución de datos 654 puede actualizar los datos almacenados en la base de datos 672 para el dispositivo de control de la diabetes 104 en base al resultado. El servidor de distribución de datos 654 puede transmitir una confirmación 752 al dispositivo de configuración 650 cuando los datos almacenados en la base de datos 672 se hayan actualizado.

Si el certificado de programa informático no está en la segunda LRC 736, el dispositivo de configuración 650 puede transmitir selectivamente una solicitud de actualización de programa informático 756 al servidor de distribución de datos 654. La solicitud de actualización de programa informático 756 puede indicar los datos (por ejemplo, una entidad de programa informático de ordenador o actualización) que se van a almacenar en el almacén de datos 532 del dispositivo de control de la diabetes 104. El servidor de distribución de datos 654 puede recuperar los datos indicados de la base de datos 672 en respuesta a la solicitud. El servidor de distribución de datos 654 puede transmitir los datos recuperados 760 para actualizar el dispositivo de control de la diabetes 104 al dispositivo de configuración 650.

El dispositivo de configuración 650 puede actualizar 764 el dispositivo de control de la diabetes 104 en base a los datos 760. Más específicamente, el dispositivo de configuración 650 puede cargar los datos 760 en el almacén de datos 532 del dispositivo de control de la diabetes 104. A continuación, el módulo procesador 504 puede ejecutar los datos 760 para controlar el funcionamiento del dispositivo de control de la diabetes 104.

Una vez completado, el dispositivo de control de la diabetes 104 puede transmitir un resultado 768 de la actualización al dispositivo de configuración 650. El resultado 768 puede indicar, por ejemplo, si la actualización fue satisfactoria. El dispositivo de configuración 650 puede transmitir una actualización de resultados 772 al servidor de distribución de datos 654. La actualización de resultados 748 puede indicar el resultado 768 de la actualización. El servidor de distribución de datos 654 puede actualizar los datos almacenados en la base de datos 672 para el dispositivo de control de la diabetes 104 en base a la actualización de resultados 748. El servidor de distribución de datos 654 puede transmitir una confirmación 776 al dispositivo de configuración 650 cuando los datos almacenados en la base de datos 672 se hayan actualizado.

Un procedimiento para proteger un dispositivo médico portátil de ejecutar una entidad de programa informático de ordenador instalada en la memoria del dispositivo médico portátil para su ejecución por el dispositivo médico portátil, comprende: recibir una lista de revocaciones desde un servidor de datos remoto en un dispositivo de configuración, incluyendo la lista de revocaciones N certificados criptográficos asociados con N entidades de programa informático de ordenador, respectivamente, que no se van a ejecutar por ninguno de un grupo de dispositivos médicos, incluyendo un dispositivo médico portátil, en el que N es un número entero mayor que o igual a cero; recibir datos desde el dispositivo médico portátil en el dispositivo de configuración, incluyendo los datos un certificado criptográfico que está asociado con una entidad de programa informático de ordenador determinada que actualmente está instalada en la memoria del dispositivo médico portátil para su ejecución por el dispositivo médico portátil; comparar el certificado criptográfico con la lista de revocaciones; y ejecutar selectivamente una función de protección por el dispositivo de configuración cuando el certificado criptográfico es el mismo que uno de los N certificados criptográficos de la lista de revocaciones.

En otros rasgos característicos, la función de protección incluye deshabilitar la ejecución de la entidad de programa informático de ordenador dada por el dispositivo médico portátil.

En otros rasgos característicos más, el dispositivo médico portátil incluye un dispositivo de control de glucemia portátil.

En otros rasgos característicos, la función de protección incluye presentar un mensaje predeterminado en una pantalla del

dispositivo médico portátil.

En otros rasgos característicos más, la función de protección incluye además pedir a un usuario que introduzca un acuse de recibo.

En otros rasgos característicos, la función de protección incluye cargar una segunda entidad de programa informático de ordenador en la memoria del dispositivo médico portátil para su ejecución por el dispositivo médico portátil, y la segunda entidad de programa informático de ordenador es diferente de la entidad de programa informático de ordenador dada.

En otros rasgos característicos más, el procedimiento comprende además: recibir datos del dispositivo en el dispositivo de configuración, incluyendo los datos del dispositivo un identificador del dispositivo médico portátil; y seleccionar la segunda entidad de programa informático de ordenador de una pluralidad de entidades de programa informático de ordenador en base al identificador.

En otros rasgos característicos, el procedimiento comprende además verificar que la segunda entidad de programa informático de ordenador no es la misma que una de los N certificados criptográficos de la lista de revocaciones.

Un procedimiento para regular la capacidad de actualización de los datos almacenados en la memoria de un dispositivo médico portátil comprende: recibir una lista de revocaciones desde un primer servidor de datos remoto en un dispositivo de configuración, incluyendo la lista de revocaciones N certificados criptográficos asociados con N dispositivos médicos portátiles, respectivamente, a los que se va a denegar el acceso a los datos accesibles por medio de un segundo servidor de datos remoto, en el que N es un número entero mayor que o igual a cero; recibir datos desde un dispositivo médico portátil en el dispositivo de configuración, incluyendo los datos un certificado criptográfico que está asociado con el dispositivo médico portátil; comparar el certificado criptográfico con la lista de revocaciones; y actualizar selectivamente el dispositivo médico portátil con datos del segundo servidor de datos remoto después de determinar que el certificado criptográfico no es el mismo que ninguno de los N certificados criptográficos de la lista de revocaciones.

En otros rasgos característicos, el primer y segundo servidores de datos remotos son diferentes.

En otros rasgos característicos más, el procedimiento comprende además, después de determinar que el certificado criptográfico no es el mismo que ninguno de los N certificados criptográficos de la lista de revocaciones: recibir una segunda lista de revocaciones desde el segundo servidor de datos remoto en un dispositivo de configuración, incluyendo la segunda lista de revocaciones M certificados criptográficos asociados con M entidades de programa informático de ordenador, respectivamente, que no se van a ejecutar por ninguno de un grupo de dispositivos médicos, incluyendo el dispositivo médico portátil, en el que M es un número entero mayor que o igual a cero, y en el que los datos incluyen además un segundo certificado criptográfico que está asociado con una entidad de programa informático de ordenador dada que está actualmente instalada en la memoria del dispositivo médico portátil para su ejecución por el dispositivo médico portátil; y comparar el segundo certificado criptográfico con la segunda lista de revocaciones.

En otros rasgos característicos, el procedimiento comprende además realizar selectivamente una función de protección por el dispositivo de configuración en respuesta a determinar que el segundo certificado criptográfico es el mismo que uno de los M certificados criptográficos en la segunda lista de revocaciones.

En otros rasgos característicos más, la función de protección incluye deshabilitar la ejecución de la entidad de programa informático de ordenador dada por el dispositivo médico portátil.

En otros rasgos característicos, la función de protección incluye presentar un mensaje predeterminado en una pantalla del dispositivo médico portátil.

En otros rasgos característicos más, la función de protección incluye además pedir a un usuario que introduzca un acuse de recibo.

En otros rasgos característicos, la función de protección incluye cargar una segunda entidad de programa informático de ordenador en la memoria del dispositivo médico portátil para su ejecución por el dispositivo médico portátil, y la segunda entidad de programa informático de ordenador es diferente de la entidad de programa informático de ordenador dada.

En otros rasgos característicos más, el procedimiento comprende además seleccionar la segunda entidad de programa informático de ordenador de una pluralidad de entidades de programa informático de ordenador en base al dispositivo médico portátil.

En otros rasgos característicos, el procedimiento comprende además verificar que la segunda entidad de programa informático de ordenador no es la misma que ninguno de los M certificados criptográficos de la segunda lista de revocaciones.

En otros rasgos característicos más, el procedimiento comprende además evitar actualizar el dispositivo médico portátil después de determinar que el certificado criptográfico es el mismo que uno de los N certificados criptográficos de la lista

de revocaciones.

En otros rasgos característicos, el dispositivo médico portátil incluye un dispositivo de control de glucemia portátil.

Las amplias enseñanzas de la divulgación se pueden implementar en una variedad de formas. Por lo tanto, si bien esta divulgación incluye ejemplos particulares, el verdadero alcance de la divulgación no debería estar así limitado, puesto que otras modificaciones resultarán evidentes para el experto en la técnica tras un estudio de los dibujos, la memoria descriptiva y las siguientes reivindicaciones.

REIVINDICACIONES

1. Un procedimiento para proteger un dispositivo médico portátil de ejecutar una entidad de programa informático de ordenador instalada en la memoria del dispositivo médico portátil para su ejecución por el dispositivo médico portátil, que comprende:

recibir una lista de revocaciones desde un servidor de datos remoto en un dispositivo de configuración, incluyendo la lista de revocaciones N certificados criptográficos asociados con N entidades de programa informático de ordenador, respectivamente, que no se van a ejecutar por ninguno de un grupo de dispositivos médicos, incluyendo un dispositivo médico portátil, en el que N es un número entero mayor que o igual a cero;

recibir datos desde el dispositivo médico portátil en el dispositivo de configuración, incluyendo los datos un certificado criptográfico que está asociado con una entidad de programa informático de ordenador dada que actualmente está instalada en la memoria del dispositivo médico portátil para su ejecución por el dispositivo médico portátil;

comparar el certificado criptográfico con la lista de revocaciones; y

ejecutar selectivamente una función de protección por el dispositivo de configuración cuando el certificado criptográfico es el mismo que uno de los N certificados criptográficos de la lista de revocaciones.

2. El procedimiento de la reivindicación 1, en el que la función de protección incluye deshabilitar la ejecución de la entidad de programa informático de ordenador dada por el dispositivo médico portátil.

3. El procedimiento de la reivindicación 1, en el que la función de protección incluye presentar un mensaje predeterminado en una pantalla del dispositivo médico portátil, en particular en el que la función de protección incluye además pedir a un usuario que introduzca un acuse de recibo.

4. El procedimiento de la reivindicación 1, en el que la función de protección incluye cargar una segunda entidad de programa informático de ordenador en la memoria del dispositivo médico portátil para su ejecución por el dispositivo médico portátil, y

en el que la segunda entidad de programa informático de ordenador es diferente de la entidad de programa informático de ordenador dada.

5. El procedimiento de la reivindicación 4, que comprende además:

recibir datos del dispositivo en el dispositivo de configuración, incluyendo los datos del dispositivo un identificador del dispositivo médico portátil; y

seleccionar la segunda entidad de programa informático de ordenador de una pluralidad de entidades de programa informático de ordenador en base al identificador, comprendiendo en particular verificar que la segunda entidad de programa informático de ordenador no es la misma que uno de los N certificados criptográficos de la lista de revocaciones.

6. Un procedimiento para regular la capacidad de actualización de los datos almacenados en la memoria de un dispositivo médico portátil, que comprende:

recibir una lista de revocaciones desde un primer servidor de datos remoto en un dispositivo de configuración, incluyendo la lista de revocaciones N certificados criptográficos asociados con N dispositivos médicos portátiles, respectivamente, a los que se les va a denegar el acceso a datos accesibles por medio de un segundo servidor de datos remoto, en el que N es un número entero mayor que o igual a cero;

recibir datos desde un dispositivo médico portátil en el dispositivo de configuración, incluyendo los datos un certificado criptográfico que está asociado con el dispositivo médico portátil;

comparar el certificado criptográfico con la lista de revocaciones; y

actualizar selectivamente el dispositivo médico portátil con los datos desde el segundo servidor de datos remoto después de determinar que el certificado criptográfico no es el mismo que cualquiera de los N certificados criptográficos de la lista de revocaciones.

7. El procedimiento de la reivindicación 6, en el que el primer y segundo servidores de datos remotos son diferentes.

8. El procedimiento de la reivindicación 6, que comprende además, después de determinar que el certificado criptográfico no es el mismo que ninguno de los N certificados criptográficos de la lista de revocaciones:

recibir una segunda lista de revocaciones desde el segundo servidor de datos remoto en un dispositivo de configuración,

incluyendo la segunda lista de revocaciones M certificados criptográficos asociados con M entidades de programa informático de ordenador, respectivamente, que no se van a ejecutar por ninguno de un grupo de dispositivos médicos, incluyendo el dispositivo médico portátil,

en el que M es un número entero mayor que o igual a cero, y

en el que los datos incluyen además un segundo certificado criptográfico que está asociado con una entidad de programa informático de ordenador dada que actualmente está instalada en la memoria del dispositivo médico portátil para su ejecución por el dispositivo médico portátil; y

comparar el segundo certificado criptográfico con la segunda lista de revocaciones.

9. El procedimiento de la reivindicación 8, que comprende además realizar selectivamente una función de protección por el dispositivo de configuración en respuesta a determinar que el segundo certificado criptográfico es el mismo que uno de los M certificados criptográficos en la segunda lista de revocaciones.

10. El procedimiento de la reivindicación 9, en el que la función de protección incluye deshabilitar la ejecución de la entidad de programa informático de ordenador dada por el dispositivo médico portátil, o incluye presentar un mensaje predeterminado en una pantalla del dispositivo médico portátil.

11. El procedimiento de la reivindicación 9, en el que la función de protección incluye cargar una segunda entidad de programa informático de ordenador en la memoria del dispositivo médico portátil para su ejecución por el dispositivo médico portátil, y

en el que la segunda entidad de programa informático de ordenador es diferente de la entidad de programa informático de ordenador dada.

12. El procedimiento de la reivindicación 11, que comprende además seleccionar la segunda entidad de programa informático de ordenador de una pluralidad de entidades de programa informático de ordenador en base al dispositivo médico portátil.

13. El procedimiento de la reivindicación 11, que comprende además verificar que la segunda entidad de programa informático de ordenador no es la misma que ninguno de los M certificados criptográficos de la segunda lista de revocaciones.

14. El procedimiento de la reivindicación 6, que comprende además evitar actualizar el dispositivo médico portátil después de determinar que el certificado criptográfico es el mismo que uno de los N certificados criptográficos de la lista de revocaciones.

15. El procedimiento de la reivindicación 6, en el que el dispositivo médico portátil incluye un dispositivo de control de glucemia portátil.

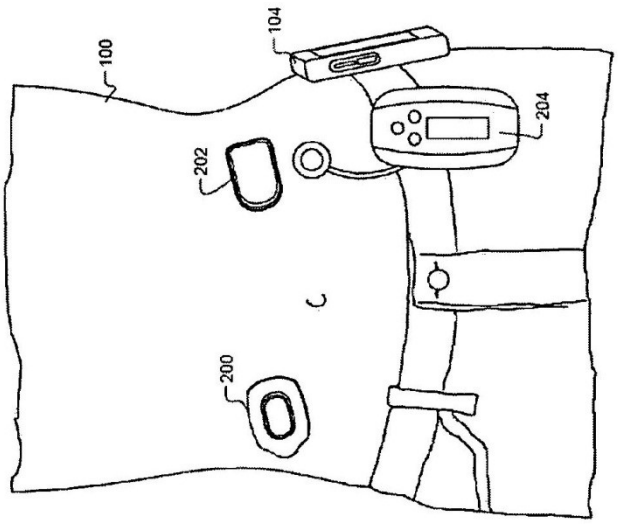

FIG. 2

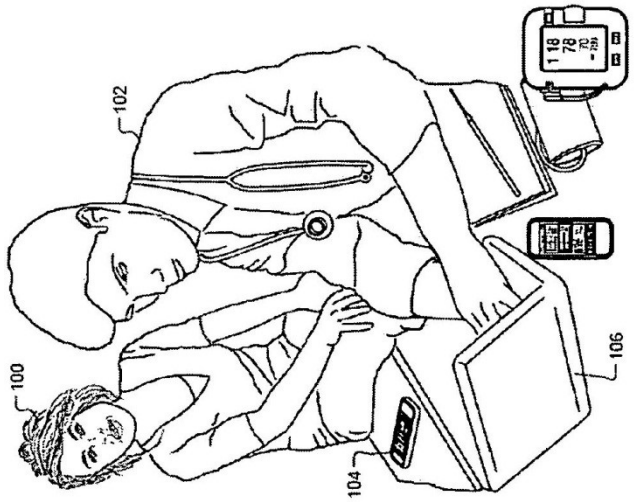

FIG. 1

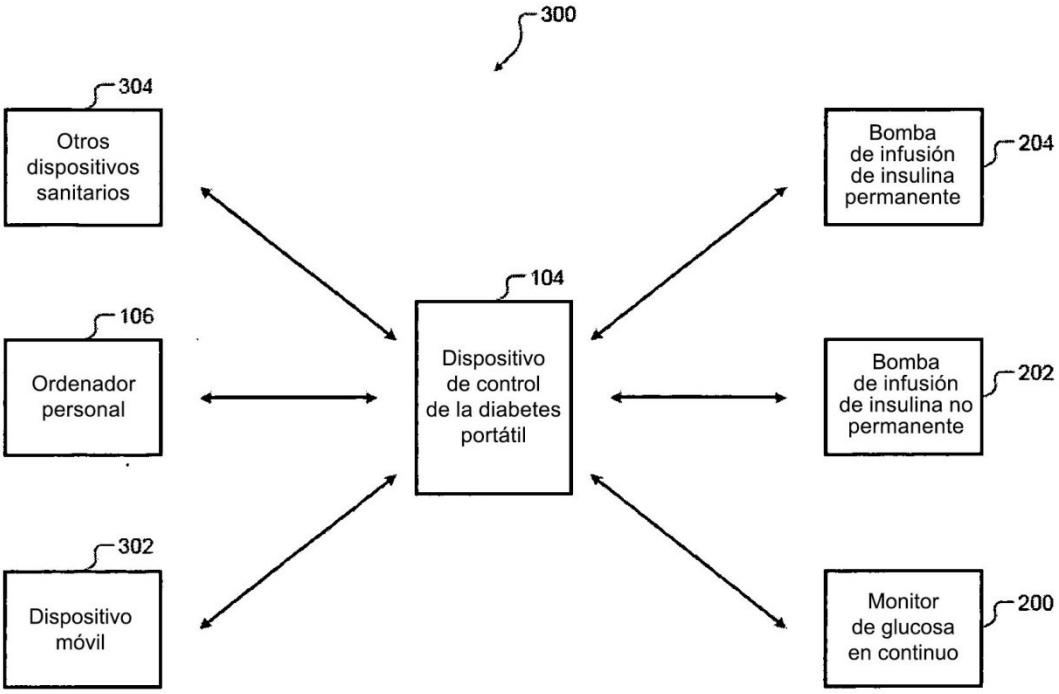
300
304
Otros dispositivos sanitarios
106
Ordenador personal
302
Dispositivo móvil
104
Dispositivo de control de la diabetes portátil
Bomba de infusión de insulina permanente
204
Bomba de infusión de insulina no permanente
202
Monitor de glucosa en continuo
200

FIG. 3

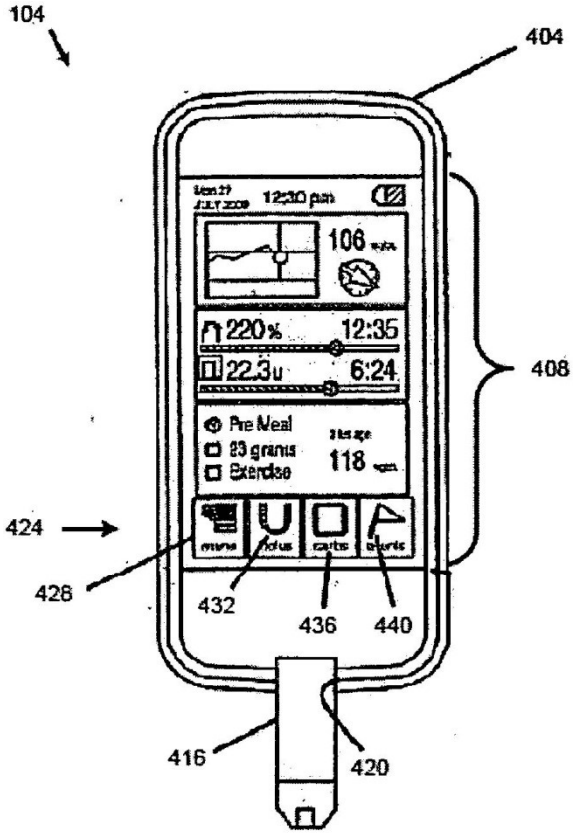
104
404
408
424
428
432
436
440
416
420
106
220%
12:35
22.3u
6:24
Pre Meal
35 grams
Exercise
118

FIG. 4

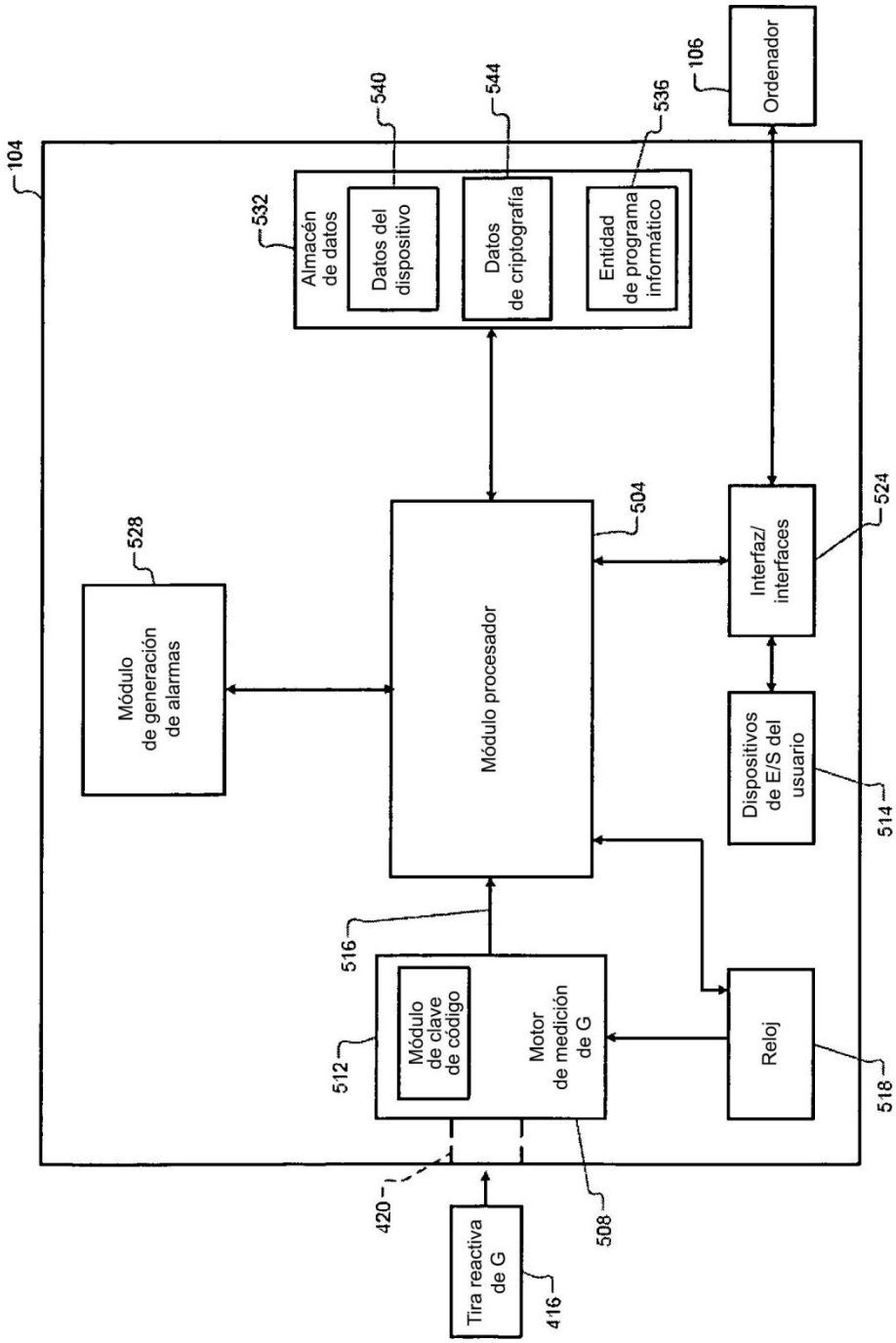
104
Ordenador
106
540
544
536
532
Almacén de datos
Datos del dispositivo
Datos de criptografía
Entidad de programa informático
528
Módulo de generación de alarmas
Módulo procesador
504
Interfaz/ interfaces
524
Dispositivos de E/S del usuario
514
516
512
Módulo de clave de código
Motor de medición de G
Reloj
518
420
508
Tira reactiva de G
416

FIG. 5

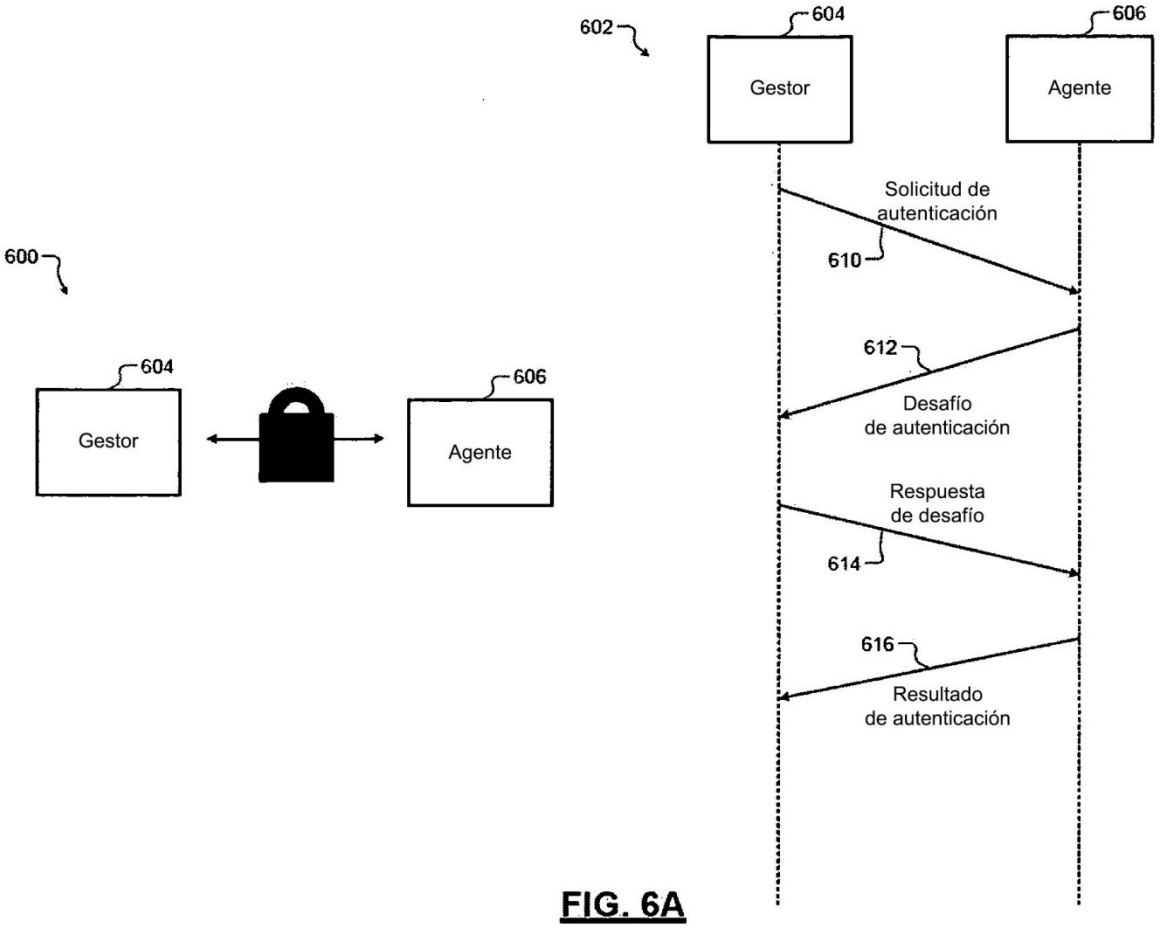
600
604
Gestor
606
Agente
602
604
Gestor
606
Agente
Solicitud de autenticación
610
612
Desafío de autenticación
Respuesta de desafío
614
616
Resultado de autenticación

FIG. 6A

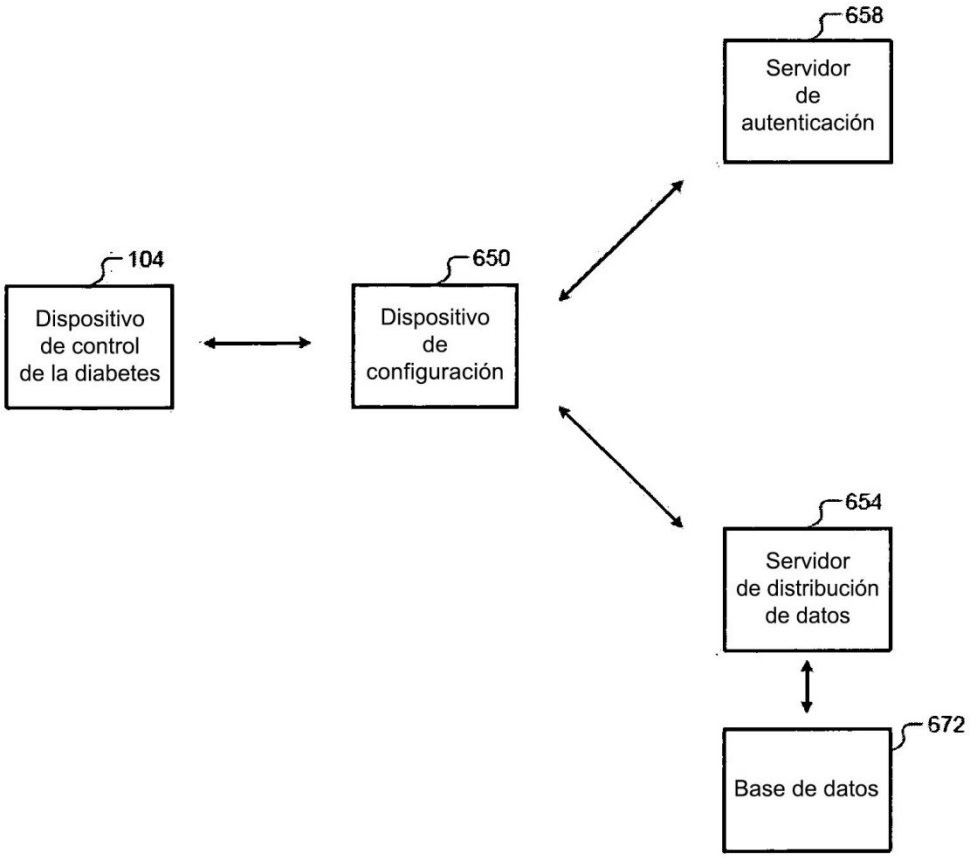
658
Servidor de autenticación
104
Dispositivo de control de la diabetes
650
Dispositivo de configuración
654
Servidor de distribución de datos
672
Base de datos

FIG. 6B

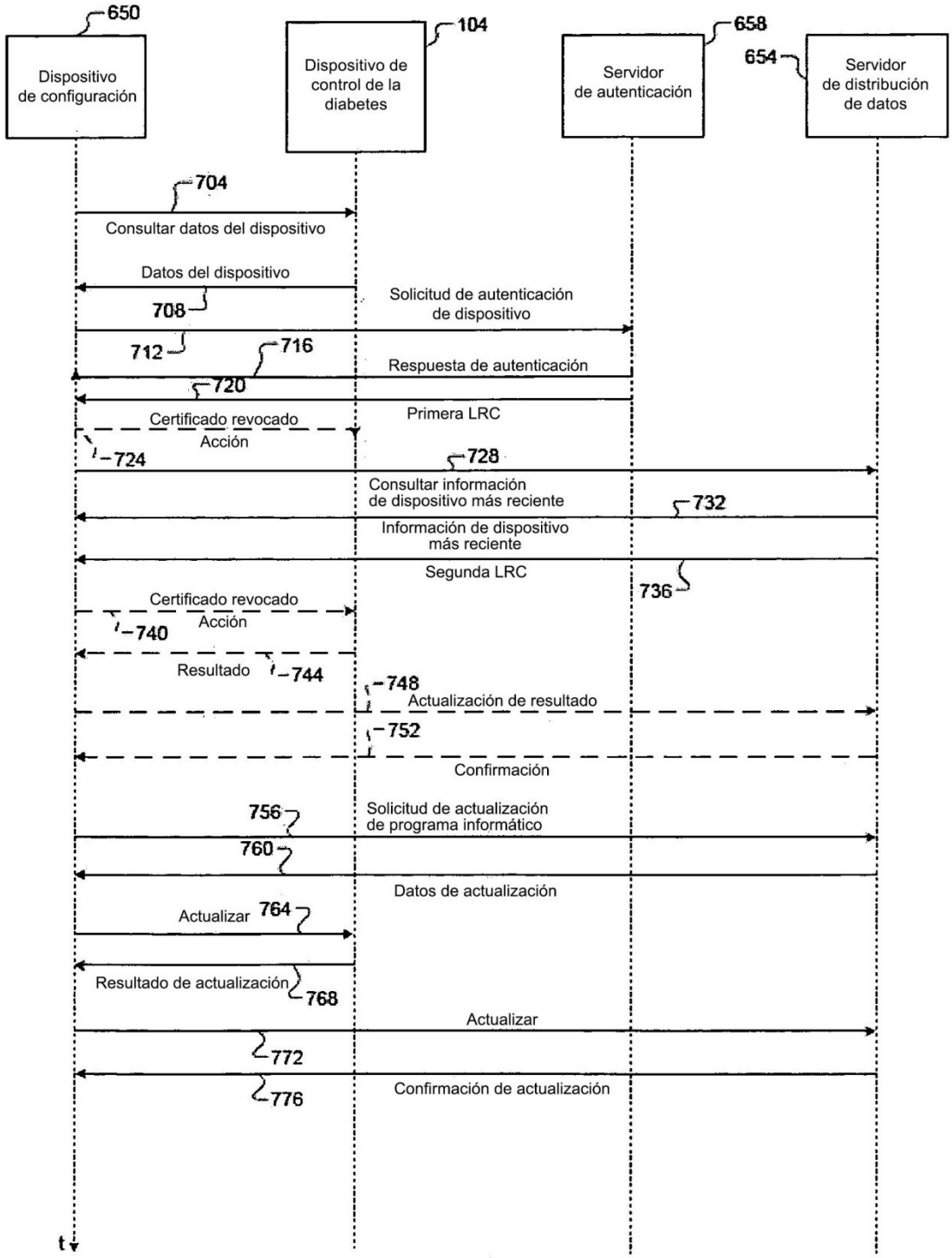

FIG. 7

16229639.1