

19



OFICINA ESPAÑOLA DE
PATENTES Y MARCAS

ESPAÑA



11 Número de publicación: **2 985 096**

51 Int. Cl.:

H04W 4/80	(2008.01)
H04W 12/00	(2011.01)
H04W 12/06	(2011.01)
A61B 5/145	(2006.01)
G16H 40/63	(2008.01)
H04L 9/40	(2012.01)
H04W 12/062	(2011.01)
H04W 12/50	(2011.01)
H04W 12/69	(2011.01)
H04W 12/71	(2011.01)

12

TRADUCCIÓN DE PATENTE EUROPEA

T3

96 Fecha de presentación y número de la solicitud europea: **19.09.2019** **E 19198266 (9)**

97 Fecha y número de publicación de la concesión europea: **15.05.2024** **EP 3627868**

54 Título: **Sistema de emparejamiento de dispositivos**

30 Prioridad:

19.09.2018 US 201816135557

45 Fecha de publicación y mención en BOPI de la traducción de la patente:
04.11.2024

73 Titular/es:

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

72 Inventor/es:

**KLEM, KURT;
CARLSON, CRAIG L.;
FORLER, JOE;
AYKROYD, TIM y
WILLIAMS, ERIC**

74 Agente/Representante:

LINAGE GONZÁLEZ, Rafael

ES 2 985 096 T3

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

DESCRIPCIÓN

Sistema de emparejamiento de dispositivos

5 La presente memoria descriptiva se refiere a sistemas y procedimientos de emparejamiento positivo de dispositivos para que los dispositivos completen un emparejamiento de comunicación inalámbrica entre un par de dispositivos inalámbricos y, más específicamente, a sistemas de emparejamiento positivo de dispositivos para completar un emparejamiento de comunicación inalámbrica autenticado entre dispositivos médicos y a procedimientos de uso de dichos sistemas.

10

Antecedentes

15 En el mercado existe una gran población de dispositivos de comunicación inalámbrica, en particular, aquellos que se comunican por medio de una comunicación inalámbrica tal como comunicación BLUETOOTH®. Cuando los dispositivos intentan emparejarse a través de un procedimiento de emparejamiento BLUETOOTH®, es posible que un dispositivo inalámbrico no previsto interfiera e, incluso, evite un emparejamiento previsto entre un dispositivo central y un dispositivo periférico.

20 En consecuencia, existe una necesidad de sistemas y procedimientos de uso alternativos que permitan el emparejamiento de comunicación inalámbrica de una manera que evite interferencias de dichos dispositivos no previstos como posibles puntos de conexión que, de otro modo, se podrían conectar a un dispositivo periférico y perjudicar un emparejamiento previsto.

25 El documento WO 2018/112417 A1 divulga un procedimiento para confirmar el emparejamiento de dispositivos habilitados para BLUETOOTH® usando una clave de confirmación. El procedimiento se realiza mediante un dispositivo informático periférico habilitado para BLUETOOTH®. El procedimiento incluye a) anunciar la disponibilidad del dispositivo informático periférico habilitado para BLUETOOTH® para el emparejamiento, b) recibir una solicitud de escaneo desde un dispositivo informático central habilitado para BLUETOOTH®, c) transmitir una respuesta de escaneo al dispositivo informático central habilitado para BLUETOOTH® en respuesta a la solicitud de escaneo, d) proporcionar un valor de confirmación al dispositivo informático central habilitado para BLUETOOTH®, e) recibir una solicitud de conexión del dispositivo informático central habilitado para BLUETOOTH®, f) establecer una conexión con el dispositivo informático central habilitado para BLUETOOTH®, g) identificar una clave de confirmación proporcionada por el dispositivo informático central habilitado para BLUETOOTH®, en el que la clave de confirmación se proporciona dentro de una característica de clave de confirmación, h) validar que la clave de confirmación es válida, y i) emparejarse con el dispositivo informático central habilitado para BLUETOOTH®.

35

Sumario

40 Un objetivo de la presente divulgación es proporcionar tecnología mejorada para sistemas y procedimientos de emparejamiento de dispositivos para que los dispositivos completen un emparejamiento de comunicación inalámbrica entre un par de dispositivos inalámbricos.

45 En las reivindicaciones independientes se define un sistema de emparejamiento de dispositivos de acuerdo con la presente invención. Los modos de realización se divulgan en las reivindicaciones dependientes.

50 En un modo de realización, un sistema de emparejamiento de dispositivos puede incluir un dispositivo periférico, un dispositivo central, uno o más procesadores, uno o más componentes de memoria acoplados de forma comunicativa al uno o más procesadores e instrucciones legibles por máquina almacenadas en el uno o más componentes de memoria. El sistema de emparejamiento de dispositivos se puede configurar para emparejar el dispositivo periférico y el dispositivo central para establecer un canal de comunicación inalámbrica emparejada entre los mismos. Las instrucciones legibles por máquina pueden provocar que el sistema de emparejamiento de dispositivos realice al menos lo siguiente cuando las ejecuta el uno o más procesadores: establecer una conexión a través de un canal de comunicación inalámbrica entre el dispositivo periférico y el dispositivo central; llevar a cabo, por el dispositivo central, un descubrimiento de características de GATT de un valor de característica de GATT de un servicio de GATT del dispositivo periférico a través del canal de comunicación inalámbrica; determinar una determinación de autenticación antes del emparejamiento de dispositivos en base a la determinación de un valor de característica de GATT central para lograr una de una determinación de coincidencia satisfactoria y una determinación de coincidencia no satisfactoria; utilizar el dispositivo central para enviar una solicitud de emparejamiento al dispositivo periférico para iniciar el emparejamiento a través del canal de comunicación inalámbrica en base al descubrimiento de características de GATT del valor de característica de GATT del servicio de GATT del dispositivo periférico. Las instrucciones pueden provocar además que el sistema de emparejamiento de dispositivos: en respuesta a la determinación de coincidencia no satisfactoria como determinación de autenticación, rechace la solicitud de emparejamiento con el dispositivo periférico; en respuesta a la determinación de coincidencia satisfactoria como determinación de autenticación, apruebe la solicitud de emparejamiento con el dispositivo periférico y envíe una respuesta de emparejamiento al dispositivo central; y empareje el dispositivo

65

central y el dispositivo periférico en base a la respuesta de emparejamiento para crear el canal de comunicación inalámbrica emparejada.

5 En otro modo de realización, el sistema de emparejamiento de dispositivos puede incluir un dispositivo periférico,
un dispositivo central, el sistema de emparejamiento de dispositivos configurado para emparejar el dispositivo
periférico y el dispositivo central para establecer un canal de comunicación inalámbrica emparejada entre los
mismos, uno o más procesadores, uno o más componentes de memoria acoplados de forma comunicativa al uno o
10 más procesadores e instrucciones antes del emparejamiento de dispositivos en base a si el rasgo característico
solicitado recibidos por el dispositivo periférico es correcto para lograr una de una determinación satisfactoria y una
determinación de coincidencia no satisfactoria; y utilizar el dispositivo central para enviar una solicitud de
emparejamiento al dispositivo periférico para iniciar el emparejamiento a través del canal de comunicación
15 inalámbrica en base al descubrimiento de características de GATT del dispositivo periférico y la determinación de
autenticación. Las instrucciones pueden provocar además que el sistema de emparejamiento de dispositivos: en
respuesta a un hallazgo incorrecto para la determinación de autenticación, rechace la solicitud de emparejamiento
con el dispositivo periférico; en respuesta a un hallazgo correcto para la determinación de autenticación, envíe una
20 respuesta de emparejamiento inicial por el dispositivo periférico que incluye una solicitud de seguridad y proceda a
una segunda determinación de autenticación; determine, en la segunda determinación de autenticación, si el
dispositivo central intercambié claves de seguridad apropiadas con el dispositivo periférico en respuesta a la
solicitud de seguridad; en respuesta a un hallazgo negativo para la segunda determinación de autenticación,
rechace la solicitud de emparejamiento con el dispositivo periférico; y, en respuesta a un hallazgo positivo para la
25 segunda determinación de autenticación, complete el emparejamiento entre el dispositivo periférico y el dispositivo
central para crear el canal de comunicación inalámbrica emparejada.

30 Aún en otro modo de realización, un sistema de emparejamiento de dispositivos puede incluir un dispositivo
periférico, un dispositivo central, el sistema de emparejamiento de dispositivos configurado para emparejar el
dispositivo periférico y el dispositivo central para establecer un canal de comunicación inalámbrica emparejada
entre los mismos, uno o más procesadores y uno o más componentes de memoria acoplados de forma
35 comunicativa al uno o más procesadores. El sistema de emparejamiento de dispositivos puede incluir además
instrucciones legibles por máquina almacenadas en el uno o más componentes de memoria que provocan que el
sistema de emparejamiento de dispositivos realice al menos lo siguiente cuando las ejecuta el uno o más
procesadores: establecer una conexión a través de un canal de comunicación inalámbrica entre el dispositivo
periférico y el dispositivo central; llevar a cabo, por el dispositivo central, un descubrimiento de características de
40 GATT de un valor de característica del dispositivo periférico a través del canal de comunicación inalámbrica; enviar
datos de autenticación desde el dispositivo central al dispositivo periférico indicativos de una primera determinación
de autenticación; utilizar el dispositivo central para enviar una solicitud de emparejamiento al dispositivo periférico
para iniciar el emparejamiento a través del canal de comunicación inalámbrica en base a la primera determinación
de autenticación; y determinar una segunda determinación de autenticación antes del emparejamiento de
45 dispositivos en base a si los datos de autenticación indican que la segunda autenticación es satisfactoria o no
satisfactoria. Las instrucciones pueden provocar además que el sistema de emparejamiento de dispositivos: en
respuesta a que la segunda determinación de autenticación sea no satisfactoria, rechace la solicitud de
emparejamiento con el dispositivo periférico; en respuesta a que la segunda determinación de autenticación sea
satisfactoria, apruebe la solicitud de emparejamiento con el dispositivo periférico y envíe una respuesta de
50 emparejamiento al dispositivo central; y empareje el dispositivo central y el dispositivo periférico en base a la
respuesta de emparejamiento para crear el canal de comunicación inalámbrica emparejada.

55 Con respecto al sistema de emparejamiento de dispositivos, se divulgan los siguientes modos de realización
adicionales.

El valor de característica de GATT del servicio de GATT del dispositivo periférico puede comprender un valor de
característica de un servicio de información del dispositivo (DIS) del dispositivo periférico.

60 Las instrucciones para determinar una determinación de autenticación antes del emparejamiento de dispositivos en
base a la determinación de un valor de característica de GATT central del dispositivo central para lograr una de una
determinación de coincidencia satisfactoria y una determinación de coincidencia no satisfactoria pueden
comprender instrucciones para: llevar a cabo, por el dispositivo periférico, un descubrimiento de características de
GATT de un valor de característica central del dispositivo central a través del canal de comunicación inalámbrica;
65 leer el valor de característica central por el dispositivo periférico para establecer el valor de característica central
como el valor de característica de GATT central; determinar la determinación de coincidencia satisfactoria en base
al valor de característica de GATT central que coincide con un valor dispuesto previamente según lo determinado

por el dispositivo periférico; y determinar la determinación de coincidencia no satisfactoria en base al valor de característica de GATT central que no coincide con un valor dispuesto previamente según lo determinado por el dispositivo periférico.

- 5 El valor de característica central puede ser uno de un valor de característica de DIS o un identificador único universal (UUID).

10 Las instrucciones para determinar una determinación de autenticación antes del emparejamiento de dispositivos en base a la determinación de un valor de característica de GATT central para lograr una de una determinación de coincidencia satisfactoria y una determinación de coincidencia no satisfactoria pueden comprender instrucciones para: usar el dispositivo central para escribir el un valor de característica central en un valor de característica del dispositivo periférico para establecer el valor de característica central como el valor de característica de GATT central; determinar la determinación de coincidencia satisfactoria en base al valor de característica de GATT central que coincide con un valor dispuesto previamente según lo determinado por el dispositivo periférico; y
15 determinar la determinación de coincidencia no satisfactoria en base al valor de característica de GATT central que no coincide con un valor dispuesto previamente según lo determinado por el dispositivo periférico.

20 El valor de característica central puede ser uno de un valor de característica de DIS o un identificador único universal (UUID).

El valor de característica de GATT central puede comprender un número de serie del dispositivo periférico presentado por el dispositivo periférico al dispositivo central.

25 El sistema de emparejamiento de dispositivos puede comprender además instrucciones para transmitir el número de serie del dispositivo periférico desde el dispositivo periférico al dispositivo central a través del canal de comunicación inalámbrica.

30 Las instrucciones pueden comprender además instrucciones para intercambiar uno o más rasgos característicos de clave de seguridad entre el dispositivo central y el dispositivo periférico antes de emparejar el dispositivo central y el dispositivo periférico.

35 El sistema de emparejamiento de dispositivos puede comprender además instrucciones para vincular el dispositivo periférico y el dispositivo central de modo que, después de emparejar el dispositivo periférico y el dispositivo central, almacenen el uno o más rasgos característicos de clave de seguridad que se intercambian.

El sistema de emparejamiento de dispositivos puede comprender además instrucciones para desconectar el dispositivo periférico y el dispositivo central después de la vinculación.

40 Las instrucciones para establecer una conexión a través de un canal de comunicación inalámbrica entre el dispositivo periférico y el dispositivo central pueden comprender además instrucciones para colocar cada uno del dispositivo periférico y el dispositivo central en un modo de emparejamiento.

45 El sistema de emparejamiento de dispositivos puede comprender además instrucciones para: poner en marcha un temporizador de autenticación al comienzo del descubrimiento de características de GATT; deshabilitar el temporizador de autenticación en respuesta a la determinación de coincidencia satisfactoria como determinación de autenticación; y mostrar una confirmación de emparejamiento en una pantalla de visualización respectiva de cada uno del dispositivo central y el dispositivo periférico después de emparejar el dispositivo central y el dispositivo periférico en base a la respuesta de emparejamiento.

50 A continuación se describen otros modos de realización.

La solicitud de seguridad puede ser para al menos uno de un rasgo característico de seguridad de intermediario (MITM) y un rasgo característico de seguridad de vinculación.

55 Para el sistema de emparejamiento de dispositivos, el rasgo característico solicitado puede ser una clave de acceso predefinida.

60 Las instrucciones para determinar la determinación de autenticación antes del emparejamiento de dispositivos en base a si el rasgo característico solicitado recibido por el dispositivo periférico es correcto para lograr una de una determinación satisfactoria y una determinación de coincidencia no satisfactoria pueden comprender instrucciones para determinar si la clave de acceso predefinida recibida por el dispositivo periférico coincide con un valor dispuesto previamente.

65 El rasgo característico solicitado puede ser una matriz de datos fuera de banda (OOB) predefinida.

Las instrucciones para determinar la determinación de autenticación antes del emparejamiento de dispositivos en

base a si el rasgo característico solicitado recibido por el dispositivo periférico es correcto para lograr una de una determinación satisfactoria y una determinación de coincidencia no satisfactoria pueden comprender instrucciones para determinar si la matriz de datos OOB predefinida recibida por el dispositivo periférico coincide con una matriz de datos OOB esperada.

5

El rasgo característico solicitado puede ser un valor predefinido de un modelo de asociación y las instrucciones para determinar la determinación de autenticación antes del emparejamiento de dispositivos en base a si el rasgo característico solicitado recibido por el dispositivo periférico es correcto para lograr una de una determinación satisfactoria y una determinación de coincidencia no satisfactoria comprenden instrucciones para determinar si el valor predefinido del modelo de asociación recibido por el dispositivo periférico coincide con un valor esperado del modelo de asociación.

10

El sistema de emparejamiento de dispositivos puede comprender además instrucciones para, en respuesta a un hallazgo negativo para la segunda determinación de autenticación, mostrar un mensaje indicativo del rechazo de la solicitud de emparejamiento en una pantalla de visualización del dispositivo periférico.

15

Para el sistema de emparejamiento de dispositivos, las instrucciones para enviar datos de autenticación desde el dispositivo central al dispositivo periférico indicativos de una primera determinación de autenticación pueden comprender instrucciones para escribir un valor por el dispositivo central en el valor de característica del dispositivo periférico, en el que un acontecimiento de escritura comprende la primera determinación de autenticación.

20

Las instrucciones para determinar una segunda determinación de autenticación antes del emparejamiento de dispositivos en base a si los datos de autenticación indican que la segunda autenticación es satisfactoria o no satisfactoria pueden comprender instrucciones para determinar si el valor escrito en el valor de característica del dispositivo periférico coincide con un valor dispuesto previamente para lograr una de una determinación de coincidencia satisfactoria indicativa de que la segunda determinación de autenticación fue satisfactoria y una determinación de coincidencia no satisfactoria indicativa de que la segunda determinación de autenticación fue no satisfactoria.

25

Las instrucciones para enviar datos de autenticación desde el dispositivo central al dispositivo periférico indicativos de una primera determinación de autenticación pueden comprender instrucciones para enviar datos de autenticación del dispositivo en respuesta a una solicitud de datos de autenticación del dispositivo desde el dispositivo periférico.

30

De acuerdo con todavía otro aspecto, se proporciona un procedimiento para emparejar dispositivos en un sistema de emparejamiento de dispositivos, comprendiendo el sistema de emparejamiento de dispositivos: un dispositivo periférico; un dispositivo central, el sistema de emparejamiento de dispositivos configurado para emparejar el dispositivo periférico y el dispositivo central para establecer un canal de comunicación inalámbrica emparejada entre los mismos; uno o más procesadores; uno o más componentes de memoria acoplados de forma comunicativa al uno o más procesadores; e instrucciones legibles por máquina almacenadas en el uno o más componentes de memoria que provocan que el sistema de emparejamiento de dispositivos realice al menos lo siguiente cuando las ejecuta el uno o más procesadores:

35

- establecer una conexión a través de un canal de comunicación inalámbrica entre el dispositivo periférico y el dispositivo central;

45

- llevar a cabo, por el dispositivo central, un descubrimiento de características de GATT de un valor de característica de GATT de un servicio de GATT del dispositivo periférico a través del canal de comunicación inalámbrica;

50

- determinar una determinación de autenticación antes del emparejamiento de dispositivos en base a la determinación de un valor de característica de GATT central para lograr una de una determinación de coincidencia satisfactoria y una determinación de coincidencia no satisfactoria;

55

- utilizar el dispositivo central para enviar una solicitud de emparejamiento al dispositivo periférico para iniciar el emparejamiento a través del canal de comunicación inalámbrica en base al descubrimiento de características de GATT del valor de característica de GATT del servicio de GATT del dispositivo periférico;

60

- en respuesta a la determinación de coincidencia no satisfactoria como determinación de autenticación, rechazar la solicitud de emparejamiento con el dispositivo periférico;

- en respuesta a la determinación de coincidencia satisfactoria como determinación de autenticación, aprobar la solicitud de emparejamiento con el dispositivo periférico y enviar una respuesta de emparejamiento al dispositivo central; y

65

- emparejar el dispositivo central y el dispositivo periférico en base a la respuesta de emparejamiento para

crear el canal de comunicación inalámbrica emparejada.

Los modos de realización divulgados anteriormente se pueden aplicar a al menos uno del dispositivo del sistema de emparejamiento de dispositivos y el procedimiento para emparejar dispositivos.

Estos y adicionales rasgos característicos proporcionados por los modos de realización descritos en el presente documento se entenderán mejor a la vista de la siguiente descripción detallada, junto con los dibujos.

Breve descripción de los dibujos

Los modos de realización expuestos en los dibujos son de naturaleza ilustrativa y ejemplar y no se pretende limitar la materia objeto definida por las reivindicaciones. La siguiente descripción detallada de los modos de realización ilustrativos se puede entender cuando se lee junto con los siguientes dibujos, donde una estructura similar se indica con números de referencia similares, y en los que:

la fig. 1 ilustra esquemáticamente un sistema de emparejamiento de dispositivos para emparejar positivamente un dispositivo central y un dispositivo periférico, de acuerdo con uno o más modos de realización mostrados y descritos en el presente documento;

la fig. 2 ilustra esquemáticamente un procedimiento de emparejamiento, que incluye una fase inicial de conexión, una fase intermedia de emparejamiento positivo y una fase final de vinculación de dispositivos, de acuerdo con uno o más modos de realización mostrados y descritos en el presente documento;

la fig. 3 ilustra esquemáticamente un procedimiento que resume etapas de ejemplo de la fase inicial de conexión de la fig. 2, de acuerdo con uno o más modos de realización mostrados y descritos en el presente documento;

la fig. 4 es un diagrama de flujo de un procedimiento que resume las etapas de ejemplo de la fase final de vinculación de dispositivos de la fig. 2, de acuerdo con uno o más modos de realización mostrados y descritos en el presente documento;

la fig. 5 es un diagrama de flujo de un procedimiento de lectura para la fase intermedia de emparejamiento positivo de la fig. 2 que puede ser un procedimiento de emparejamiento positivo basado en lectura de características y/o servicio de perfil de atributos genéricos (GATT) para autenticar un inicio de emparejamiento antes de permitir la presentación de una respuesta de emparejamiento, de acuerdo con uno o más modos de realización mostrados y descritos en el presente documento;

la fig. 6 es un diagrama de flujo de un procedimiento de escritura para la fase intermedia de emparejamiento positivo de la fig. 2 que puede ser un procedimiento de emparejamiento positivo basado en escritura de características y/o servicio de GATT para autenticar un inicio de emparejamiento antes de permitir la presentación de una respuesta de emparejamiento, de acuerdo con uno o más modos de realización mostrados y descritos en el presente documento;

la fig. 7 es un diagrama de flujo de otro procedimiento de escritura para la fase intermedia de emparejamiento positivo de la fig. 2 y, en particular, un procedimiento de emparejamiento positivo basado en escritura para autenticar un emparejamiento antes del inicio del emparejamiento, de acuerdo con uno o más modos de realización mostrados y descritos en el presente documento;

la fig. 8 es un diagrama de flujo de un procedimiento de modelo de asociación para la fase intermedia de emparejamiento positivo de la fig. 2, y muestra un ejemplo de un procedimiento de emparejamiento positivo basado en clave de acceso para autenticar un inicio de emparejamiento antes de permitir la presentación de una respuesta de emparejamiento, de acuerdo con uno o más modos de realización mostrados y descritos en el presente documento;

la fig. 9 es un diagrama de flujo de un procedimiento de autenticación de rasgo característico de seguridad fuera de banda (OOB) para la fase intermedia de emparejamiento positivo de la fig. 2 y, en particular, un procedimiento de emparejamiento positivo basado en OOB para autenticar un inicio de emparejamiento antes de permitir la presentación de una respuesta de emparejamiento, de acuerdo con uno o más modos de realización mostrados y descritos en el presente documento;

la fig. 10 es un diagrama de flujo de un procedimiento de autenticación del dispositivo para la fase intermedia de emparejamiento positivo de la fig. 2 y, en particular, un procedimiento de emparejamiento positivo basado en autenticación para autenticar un emparejamiento antes del inicio del emparejamiento, de acuerdo con uno o más modos de realización mostrados y descritos en el presente documento;

la fig. 11 ilustra esquemáticamente un sistema para implementar procedimientos basados en ordenador y programa informático para utilizar los sistemas y procedimientos de emparejamiento positivo de la fig. 1-10, de acuerdo con uno o más modos de realización mostrados y descritos en el presente documento.

5 Descripción detallada

En general en referencia a las figuras, los modos de realización de la presente divulgación se dirigen a sistemas de emparejamiento de dispositivos para emparejar dispositivos a través de una comunicación inalámbrica emparejada, que puede estar cifrada, en base al éxito de procedimientos de autenticación de emparejamiento alternativos y a procedimientos de uso de dichos sistemas. Por ejemplo, hay múltiples dispositivos médicos disponibles y proporcionados para múltiples mercados mundiales y se pueden configurar a través de un esquema de comunicación inalámbrica, tal como una comunicación BLUETOOTH® siguiendo una especificación de BLUETOOTH® Core V4.0 y superior, para emparejarse entre sí. Dichos dispositivos médicos los pueden utilizar usuarios tales como personas diabéticas para controlar más eficazmente sus afecciones diabéticas, tal como se describe con más detalle a continuación. Sin embargo, cuando un par de dichos dispositivos médicos que incluyen un dispositivo periférico y un dispositivo central intentan emparejarse a través del esquema de comunicación inalámbrica, existe la posibilidad de que un dispositivo inalámbrico no previsto pueda interferir con e, incluso, pueda evitar el emparejamiento deseado de dispositivos entre el dispositivo periférico y el dispositivo central. Los modos de realización de los sistemas del presente documento describen mecanismos y esquemas de autenticación antes del emparejamiento de dispositivos que pueden ayudar a filtrar previamente dichos dispositivos no previstos para eliminar o reducir la posibilidad de que dispositivos no previstos se conecten con el dispositivo periférico y perjudiquen el emparejamiento deseado entre el dispositivo periférico previsto y el dispositivo central previsto. Asimismo, los mecanismos y esquemas de autenticación descritos en el presente documento que se producen antes del emparejamiento de dispositivos ayudan a mejorar las tecnologías asociadas y la eficacia del procesamiento al acelerar los procedimientos de emparejamiento y reducir el tiempo de emparejamiento para dichos procesamientos al confirmar el emparejamiento entre dispositivos antes de iniciar etapas de emparejamiento que requieren mucho tiempo, de modo que las comprobaciones de confirmación de autenticación de emparejamiento tengan lugar antes de una primera solicitud de emparejamiento. Como se describirá con más detalle en los modos de realización a continuación, dicha solicitud de emparejamiento puede utilizar la comprobación de confirmación de autenticación de emparejamiento para dar como resultado un rechazo del emparejamiento en base a una autenticación no satisfactoria o bien una presentación de una respuesta de emparejamiento positiva en base a una autenticación satisfactoria.

Ahora se hará referencia en detalle a modos de realización de los sistemas de emparejamiento de dispositivos que incluyen dichos mecanismos de autenticación y en los dibujos adjuntos se ilustran ejemplos de dichos sistemas. En la medida de lo posible, se usarán los mismos números de referencia a lo largo de los dibujos para referirse a las mismas piezas o piezas similares. En el presente documento se describirán con más detalle diversos modos de realización de los sistemas de configuración del administrador de datos de dispositivos médicos con referencia específica a los dibujos adjuntos.

En referencia a la fig. 1, un sistema de emparejamiento de dispositivos 100 incluye un par de dispositivos, siendo uno un dispositivo periférico 102 y el otro un dispositivo central 104. El dispositivo periférico 102 y el dispositivo central 104 pueden ser un par de dispositivos médicos. Cada dispositivo médico puede ser un medidor de glucemia, un monitor continuo de glucosa, una bomba de insulina, un dispositivo de bienestar o un dispositivo médico similar. A modo de ejemplo y no como limitación, un dispositivo de bienestar puede ser un dispositivo configurado para mejorar el bienestar de un individuo a través del seguimiento de datos de bienestar asociados con la salud y el bienestar del individuo y/o la monitorización de la actividad del individuo. Dichos datos de bienestar pueden incluir, por ejemplo, datos indicativos de constantes vitales que incluyen frecuencia cardíaca, calorías consumidas y quemadas y niveles de colesterol. La actividad monitorizada del individuo puede incluir datos indicativos de un número de pasos dados en un periodo de tiempo u otra actividad física llevada a cabo por el individuo, tal como correr, montar en bicicleta o hacer senderismo.

Además, el sistema de emparejamiento de dispositivos 100 incluye al menos un procesador y una memoria acoplada de forma comunicativa al procesador, tal como el uno o más procesadores 1104 y el uno o más componentes de memoria 1106 como se describen con respecto a la fig. 11 con más detalle a continuación. El sistema de emparejamiento de dispositivos 100 incluye instrucciones legibles por máquina almacenadas en la memoria que provocan que el sistema de emparejamiento de dispositivos 100 realice una o más instrucciones cuando las ejecuta el procesador.

En referencia de nuevo a la fig. 1, el dispositivo periférico 102 y el dispositivo central 104 se pueden comunicar a través de un protocolo inalámbrico 106, tal como un protocolo de atributos (ATT) usado para la comunicación BLUETOOTH®. La comunicación BLUETOOTH® permite que los dispositivos se comuniquen sin un dispositivo central tal como un enrutador o punto de acceso. La comunicación BLUETOOTH® también utiliza un rasgo característico de baja energía denominado BLUETOOTH® Low Energy (BLE), de modo que la comunicación BLUETOOTH® se pueda usar sin requerir mucha energía de los dispositivos que usan la comunicación BLUETOOTH®.

Como ejemplo no limitante, el dispositivo periférico 102 incluye un perfil de atributos genéricos (GATT) usado para la comunicación BLUETOOTH®. El GATT para un dispositivo que usa comunicación BLUETOOTH® es un perfil de BLUETOOTH® que actúa como una especificación de interfaz para definir los datos que tiene un dispositivo, qué puede hacer otro dispositivo de conexión con dichos datos a través de una comunicación y conexión BLUETOOTH®, y cómo debe responder el dispositivo con el GATT cuando el dispositivo de conexión actúa en los datos.

El GATT del dispositivo periférico 102 incluye una tabla de atributos que es una tabla de datos accesible por otros dispositivos conectados mediante diversos procedimientos de acceso. El GATT del dispositivo periférico 102 incluye los servicios 108, 114, las características 110A, 110B, 116A, 116B y los descriptores 118A, 118B como tipos de atributos de la tabla de atributos. Cada uno de los atributos descritos en el presente documento incluye un tipo identificado mediante un identificador único universal (UUID), y se pueden definir uno o más atributos mediante el BLUETOOTH® Special Interests Group (SIG), que es el organismo de normas técnicas para BLUETOOTH®. Dichos atributos definidos pueden tener UUID de 16 bits de longitud. Se pueden diseñar de forma personalizada uno o más de otros atributos para un dispositivo y tener UUID de 128 bits de longitud. Si bien un servicio debe tener una o más características, que son uno o más valores usados por el servicio, no es necesario que una característica tenga un descriptor. Para el GATT del dispositivo periférico 102, el servicio 108 incluye las características 110A, 110B, que incluyen respectivamente los descriptores 112A, 112B. Adicionalmente, el servicio 114 incluye las características 116A, 116B, que incluyen respectivamente los descriptores 118A, 118B.

A modo de ejemplo y no como limitación, los servicios 108, 114 son representativos respectivamente de un rasgo característico particular del dispositivo periférico 102, tal como un rasgo característico de equipo informático que puede ser un botón o un sensor particular. El servicio 108 puede ser, por ejemplo, un servicio de información del dispositivo (DIS) que incluye diversa información sobre el dispositivo periférico 102, que incluye datos del fabricante y del número de serie e información adicional con respecto a aspectos particulares del dispositivo. Un DIS es un servicio definido por el BLUETOOTH® SIG.

Las características 110A, 110B, 116A, 116B son representativas de datos de características que se refieren a un estado interno particular del dispositivo periférico 102, un estado ambiental que es medible por el dispositivo periférico 102 tal como a través de un sensor del dispositivo periférico 102, o datos de configuración tales como establecer una frecuencia a la que realizar dichas mediciones del sensor. Como ejemplo no limitante, un nivel de la batería puede ser datos representativos del estado interno, mientras que la temperatura puede ser datos representativos del estado ambiental.

En un modo de realización, las características 110A, 110B, 116A, 116B también proporcionan información con respecto a cómo dichos datos de características se ponen a disposición de un dispositivo de conexión, tal como el dispositivo central 104, para usarlos a través de un emparejamiento y/o comunicación BLUETOOTH®. Las características 110A, 110B, 116A, 116B pueden incluir una o más partes, tales como un tipo, un valor, una o más propiedades y/o uno o más permisos. Como ejemplo no limitante, un valor de UUID puede ser indicativo de qué tipo particular de característica puede ser un atributo, y el valor puede ser representativo del valor de un elemento de datos de estado asociado con la característica. La una o más propiedades pueden ser definitivas de las acciones que otro dispositivo, tal como el dispositivo central 104, puede tomar con una característica de, por ejemplo, el dispositivo periférico 102, a través de un emparejamiento y/o comunicación BLUETOOTH®, tal como lectura, escritura o notificación con respecto a la característica.

La lectura de una característica por el dispositivo central 104 permite transferir un valor de característica actual desde una tabla de atributos del dispositivo periférico 102 al dispositivo central 104. La escritura de una característica por el dispositivo central 104 permite que el dispositivo central 104 escriba y cambie el valor de la característica en la tabla de estado del dispositivo periférico 102. La notificación permite proporcionar un tipo de mensaje especial que un dispositivo, tal como el dispositivo periférico 102, puede enviar a un dispositivo de conexión, tal como el dispositivo central 104, cuando cambia un valor de característica o tras un intervalo de tiempo controlado periódicamente. El uno o más permisos se asocian con rasgos característicos de seguridad y pueden describir una o más condiciones de seguridad requeridas antes de otorgar acceso de lectura o escritura de características a un dispositivo, tal como el dispositivo central 104.

En un modo de realización, los descriptores 112A, 112B, 118A, 118B del GATT del dispositivo periférico 102 incluyen metadatos que pueden aumentar uno o más detalles que se refieren a las respectivas características 110A, 110B, 116A, 116B a las que pertenecen los descriptores 112A, 112B, 118A, 118B o permitir la configuración de un comportamiento de las respectivas características 110A, 110B, 116A, 116B, tal como habilitar o deshabilitar mensajes de notificación.

Como ejemplo no limitante, el dispositivo central 104 también incluye un perfil de atributos genéricos (GATT) usado para la comunicación BLUETOOTH®. El GATT del dispositivo central 104 incluye una tabla de atributos que es una tabla de datos accesible por otros dispositivos conectados mediante diversos procedimientos de acceso. El GATT del dispositivo central 104 incluye los servicios 120, 126, las características 122A, 122B, 128 y los descriptores

124A, 124B como tipos de atributos de la tabla de atributos. El servicio 120 incluye las características 122A, 122B, que incluyen respectivamente los descriptores 124A, 124B. El servicio 126 incluye la característica 128.

5 A modo de ejemplo y no como limitación, los servicios 120, 126 son representativos respectivamente de un rasgo característico particular del dispositivo central 104, tal como un rasgo característico de equipo informático que puede ser un botón o un sensor particular. El servicio 120 puede ser, por ejemplo, un DIS que incluye diversa información sobre el dispositivo central 104, que incluye datos del fabricante y del número de serie.

10 Las características 122A, 122B, 128 son representativas de datos de características que se refieren a un estado interno particular del dispositivo central 104, un estado ambiental que es medible por el dispositivo central 104 tal como a través de un sensor, o datos de configuración tales como establecer una frecuencia a la que realizar dichas mediciones del sensor. En un modo de realización, las características 122A, 122B, 128 también proporcionan información con respecto a cómo dichos datos de características se ponen a disposición de un dispositivo de conexión para usarlos a través de un emparejamiento y/o comunicación BLUETOOTH®. Las características 122A, 15 122B, 128 pueden incluir una o más partes, tales como un tipo, un valor, una o más propiedades y/o uno o más permisos similares a los descritos anteriormente con respecto a las características 110A, 110B, 116A, 116B del GATT del dispositivo periférico 102.

20 En un modo de realización, los descriptores 124A, 124B del GATT del dispositivo central 104 incluyen metadatos que pueden aumentar uno o más detalles que se refieren a las respectivas características 122A, 122B a las que pertenecen los descriptores 124A, 124B o permitir la configuración de un comportamiento de las respectivas características 122A, 122B.

25 La fig. 2 ilustra un procedimiento de emparejamiento y vinculación de dispositivos 200 entre el dispositivo periférico 102 y el dispositivo central 104, que incluye una fase inicial de conexión 202, una fase intermedia de emparejamiento positivo 204 y una fase final de vinculación de dispositivos 206. En al menos un modo de realización, uno o más procesadores 1104 se configuran para realizar el procedimiento de emparejamiento de dispositivos 200 desde la fase inicial de conexión 202 hasta la fase final de vinculación de dispositivos 206, como se describe con más detalle a continuación. El uno o más procesadores 1104 se configuran para realizar, por ejemplo, etapas de la fase inicial de conexión 202 como se describe además con respecto a un procedimiento de descubrimiento de dispositivos 302 de la fig. 3, la fase intermedia de emparejamiento positivo 204 como se describe además con respecto a modos de realización representados como procedimientos de emparejamiento positivo 504-1004 de las figs. 5-10, y una fase final de vinculación de dispositivos 206 como se describe además con respecto a un procedimiento de vinculación 406 de la fig. 4.

35 La fig. 3 ilustra un procedimiento de descubrimiento de dispositivos 302 que se puede implementar como la fase inicial de conexión 202 de la fig. 2. Como ejemplo no limitante, tanto el dispositivo periférico 102 como el dispositivo central 104 se colocan en modo de emparejamiento por, por ejemplo, un usuario para iniciar el procedimiento de descubrimiento de dispositivos 302. En el modo de emparejamiento, el dispositivo periférico 102 anuncia paquetes de datos en el bloque 304. En un modo de realización, a través del uso de un perfil de acceso genérico (GAP) de la arquitectura BLUETOOTH® asociada, un usuario puede seleccionar una opción de modo de emparejamiento en el dispositivo periférico de modo que el dispositivo periférico 102 anuncie los paquetes de datos emitiendo paquetes de datos periódicamente, que pueden ser pequeños paquetes de datos. Como ejemplo no limitante, GAP es una capa del apilamiento de la arquitectura BLUETOOTH® que determina la topología de red del sistema de la arquitectura BLUETOOTH®. Los paquetes de datos anunciados por GAP incluyen información sobre el dispositivo periférico 102, que pueden ser, por ejemplo, datos de fabricación de la configuración del dispositivo del dispositivo periférico 102.

50 Otros dispositivos, tales como el dispositivo central 104, que buscan dispositivos con los que conectarse actúan como dispositivos de escaneo configurados para escanear, recibir y procesar los paquetes de datos que se anuncian. Como ejemplo no limitante, se puede hacer referencia al dispositivo periférico 102 como un dispositivo periférico GAP, y se puede hacer referencia al dispositivo central 104 como un dispositivo central GAP configurado para iniciar la conexión con el dispositivo periférico GAP.

55 En el bloque 306, el dispositivo central 104 escanea y recibe los paquetes de datos anunciados del dispositivo periférico 102. El dispositivo central 104 rechaza y filtra paquetes de datos de dispositivos con los que el dispositivo central 104 no está interesado en comunicarse, tales como dispositivos de un tipo particular no deseado como se anuncia en sus respectivos paquetes de datos. En al menos un modo de realización, un usuario selecciona una opción del menú del dispositivo central 104 para descubrir dispositivos, y el dispositivo central 104 entra en un modo de escaneo para descubrir dispositivos y envía una solicitud de escaneo. Los dispositivos descubiertos por el dispositivo central 104 que envían una respuesta de escaneo pueden estar dentro de un determinado alcance del dispositivo central 104 en base a, por ejemplo, una medición del indicador de intensidad de la señal recibida (RSSI) de un dispositivo que se puede descubrir, tal como el dispositivo periférico 102.

65 En el bloque 308, el dispositivo periférico se selecciona de la lista de dispositivos descubiertos del dispositivo central 104. En al menos un modo de realización, un usuario puede seleccionar el dispositivo periférico de la lista

de dispositivos descubiertos en una pantalla de visualización del dispositivo central 104 si, por ejemplo, se encuentran múltiples dispositivos. En el bloque 310, el dispositivo central 104 envía una solicitud de conexión al dispositivo periférico 102 seleccionado. En el bloque 312 se establece una conexión entre el dispositivo central 104 y el dispositivo periférico 102. Después de que se establezca la conexión, el dispositivo central 104 y el dispositivo periférico 102 pueden continuar a la fase intermedia de emparejamiento positivo 204 para emparejar los dispositivos a través del intercambio de información que es necesaria para establecer una conexión cifrada emparejada.

Después del emparejamiento a través de la fase intermedia de emparejamiento positivo 204, que se describe con más detalle a continuación con respecto a los modos de realización de procedimientos de emparejamiento positivo 504-1004 de las figs. 5-10, el dispositivo central 104 y el dispositivo periférico 102 pueden realizar un procedimiento de vinculación 406 (fig. 4) como se refleja a través de la fase final de vinculación de dispositivos 206 de la fig. 2. En el procedimiento de vinculación 406, la información de la fase intermedia de emparejamiento positivo 204 se almacena en el dispositivo central 104 y el dispositivo periférico 102, de modo que la fase intermedia de emparejamiento positivo 204 no necesite repetirse cada vez que la conexión del dispositivo central 104 y el dispositivo periférico 102 esté en curso.

La fig. 4 ilustra al menos un modo de realización del procedimiento de vinculación 406. En el bloque 408, el emparejamiento entre el dispositivo periférico 102 y el dispositivo central 104 se completa después de que la fase intermedia de emparejamiento positivo 204 concluya para avanzar a la fase final de vinculación de dispositivos 206 de la fig. 2. En el bloque 410 se puede producir una configuración del dispositivo periférico 102 ahora emparejado en base a la finalización del emparejamiento entre el dispositivo central 104 y el dispositivo periférico 102. Por ejemplo, el dispositivo central 104 puede escribir en determinadas características del dispositivo periférico 102 emparejado para controlar y configurar además el dispositivo periférico 102.

En el bloque 412, el dispositivo periférico 102 y el dispositivo central 104 muestran una confirmación de emparejamiento en las respectivas pantallas de visualización para indicar un emparejamiento satisfactorio entre el dispositivo periférico 102 y el dispositivo central 104. En el bloque 414 se completa una vinculación de dispositivos entre el dispositivo periférico 102 y el dispositivo central 104. En al menos un modo de realización, la vinculación de dispositivos permite que la información de la fase intermedia de emparejamiento positivo 204 se almacene en el dispositivo central 104 y el dispositivo periférico 102, de modo que la fase intermedia de emparejamiento positivo 204 no necesite repetirse cada vez que la conexión del dispositivo central 104 y el dispositivo periférico 102 esté en curso después de un emparejamiento satisfactorio. En el bloque 416, el dispositivo central 104 y el dispositivo periférico 102 se pueden desconectar entre sí desde cualquier lado.

En referencia de nuevo a la fig. 2, la fase intermedia de emparejamiento positivo 204 se establece entre la fase inicial de conexión 202 de la fig. 3 y la fase final de vinculación de dispositivos 206. La fase inicial de conexión 202 se describe con más detalle anteriormente con respecto al procedimiento de descubrimiento de dispositivos 302 de la fig. 3, y la fase final de vinculación de dispositivos 206 se describe con más detalle anteriormente con respecto al procedimiento de vinculación 406 de la fig. 4. La fase intermedia de emparejamiento positivo 204 se describe con más detalle a continuación con respecto a los modos de realización alternativos representados respectivamente como la pluralidad de procedimientos de emparejamiento positivo 504-1004 de las figs. 5-10.

En al menos un modo de realización, el sistema de emparejamiento de dispositivos 100 se configura para implementar la pluralidad de procedimientos de emparejamiento positivo 504-1004 de las figs. 5-10 e incluye el dispositivo periférico 102, el dispositivo central 104, uno o más procesadores 1104, uno o más componentes de memoria 1106 acoplados de forma comunicativa al uno o más procesadores 1104, como se describe con más detalle a continuación, e instrucciones legibles por máquina almacenadas en el uno o más componentes de memoria 1106 que provocan que el sistema de emparejamiento de dispositivos 100 realice e implemente al menos la pluralidad de procedimientos de emparejamiento positivo 504-1004 cuando las ejecutan el uno o más procesadores 1104. El sistema de emparejamiento de dispositivos 100 se configura además para emparejar el dispositivo periférico 102 y el dispositivo central para establecer un canal de comunicación inalámbrica emparejada entre los mismos.

Como ejemplo no limitante, las figs. 5-6 ilustran respectivamente procedimientos de emparejamiento positivo basados en GATT como un procedimiento de emparejamiento positivo basado en lectura de GATT 504 en la fig. 5 y un procedimiento de emparejamiento positivo basado en escritura de GATT 604 en la fig. 6, descritos con más detalle a continuación y para que los implemente, por ejemplo, el sistema de emparejamiento de dispositivos 100. Como se describe con más detalle a continuación con respecto a los modos de realización de las figs. 5-6, las instrucciones legibles por máquina del sistema de emparejamiento de dispositivos 100 pueden incluir instrucciones para establecer una conexión a través de un canal de comunicación inalámbrica entre el dispositivo periférico 102 y el dispositivo central 104; llevar a cabo, por el dispositivo central 104, un descubrimiento de características de GATT de un valor de característica GATT de un servicio de GATT (tal como de un servicio de información del dispositivo (DIS)) del dispositivo periférico 102 a través del canal de comunicación inalámbrica; determinar una determinación de autenticación antes del emparejamiento de dispositivos en base a la determinación de un valor de característica de GATT central (tal como un valor de característica de DIS o UUID) para lograr una de una

determinación de coincidencia satisfactoria y una determinación de coincidencia no satisfactoria; y utilizar el dispositivo central 104 para enviar una solicitud de emparejamiento al dispositivo periférico 102 para iniciar el emparejamiento a través del canal de comunicación inalámbrica en base al descubrimiento de características de GATT del valor de característica de GATT del servicio de GATT del dispositivo periférico 102. En respuesta a la
 5 determinación de coincidencia no satisfactoria como determinación de autenticación, la instrucción puede ser rechazar la solicitud de emparejamiento con el dispositivo periférico 102. Las instrucciones pueden ser además, en respuesta a la determinación de coincidencia satisfactoria como determinación de autenticación, aprobar la solicitud de emparejamiento con el dispositivo periférico 102 y enviar una respuesta de emparejamiento al
 10 dispositivo central 104, y emparejar el dispositivo central 104 y el dispositivo periférico 102 en base a la respuesta de emparejamiento para crear el canal de comunicación inalámbrica emparejada. En modos de realización, el valor de característica de GATT del servicio de GATT del dispositivo periférico 102 comprende un valor de característica de un servicio de información del dispositivo (DIS) del dispositivo periférico 102.

En referencia a la fig. 5, se ilustra un procedimiento 504 de emparejamiento positivo basado en lectura de GATT, correspondiente a un modo de realización de la fase intermedia de emparejamiento positivo 204 de la fig. 2. En particular, la fig. 5 ilustra un procedimiento de emparejamiento positivo basado en lectura de GATT para autenticar un inicio de emparejamiento antes de permitir la presentación de una respuesta de emparejamiento, como se describe con más detalle a continuación.

En el bloque 506 se inicia un descubrimiento de servicio de GATT y en el bloque 508 se inicia un descubrimiento de características de GATT de subconjunto. A modo de ejemplo y no como limitación, el dispositivo central 104 inicia un descubrimiento de servicio de GATT con respecto a uno o más servicios de GATT particulares del dispositivo periférico 102 en el bloque 506. En el bloque 508, el dispositivo central 104 inicia además un descubrimiento de servicio de GATT con respecto a una o más características de GATT particulares de los servicios de GATT descubiertos del dispositivo periférico 102 del bloque 506.

En el bloque 510, como comprobación de confirmación de autenticación de emparejamiento, el dispositivo periférico 102 recibe y lee un valor del dispositivo central 104 (tal como del DIS del dispositivo central 104). En el bloque 512, el dispositivo central envía una solicitud de emparejamiento al dispositivo periférico para iniciar el emparejamiento en base a los servicios de GATT descubiertos y las características de GATT de los bloques 506-508 y la comprobación de confirmación de autenticación de emparejamiento del bloque 510. En un modo de realización se rechaza una solicitud de emparejamiento cuando se realiza antes de la comprobación de confirmación de autenticación de emparejamiento del bloque 510.

El dispositivo periférico 102 puede iniciar un descubrimiento de servicio de GATT con respecto al dispositivo central 104 y un descubrimiento de características de GATT con respecto a una o más características de GATT particulares del dispositivo central 104. En al menos un modo de realización, el dispositivo periférico 102 confirma la recepción y una lectura de al menos un valor de característica de GATT central descubierta, tal como un valor de característica de DIS o UUID del dispositivo central 104. En al menos un modo de realización, las instrucciones legibles por máquina ejecutadas por el uno o más procesadores 1104 pueden provocar que el sistema de emparejamiento de dispositivos 100 lleve a cabo además, por el dispositivo periférico 102, un descubrimiento de características de GATT de un valor de característica central de un servicio (tal como el DIS) del dispositivo central 104 a través del canal de comunicación inalámbrica, lea el valor de característica central por el dispositivo periférico 102 para establecer el valor de característica central como el valor de característica de GATT central, y determine la determinación de coincidencia satisfactoria en base al valor de característica de GATT central que coincide con un valor dispuesto previamente según lo determinado por el dispositivo periférico 102, y determine la determinación de coincidencia no satisfactoria en base al valor de característica de GATT central que no coincide con un valor dispuesto previamente según lo determinado por el dispositivo periférico 102.

Como ejemplo no limitante, en el bloque 516, el procedimiento de emparejamiento positivo basado en lectura de GATT 504 determina, a través de uno o más procesadores 1104, por ejemplo, si el al menos un valor de característica de GATT central leído del dispositivo central 104 coincide con un valor dispuesto previamente. En al menos un modo de realización, el valor dispuesto previamente lo puede introducir un desarrollador con respecto al GATT del dispositivo periférico 102. De lo contrario, la autenticación de emparejamiento falla y el dispositivo periférico 102 rechaza el emparejamiento y se desconecta del dispositivo central 104 en el bloque 514. Si se determina una coincidencia en el bloque 516, el procedimiento de emparejamiento positivo basado en lectura de GATT 504 continúa al bloque 518. En el bloque 518, el dispositivo periférico 102 envía una respuesta de emparejamiento al dispositivo central 104. En al menos un modo de realización, la respuesta de emparejamiento es indicativa de un emparejamiento autenticado y no requiere rasgos característicos de seguridad requeridos adicionales para el emparejamiento, tales como de intermediario (MITM) y de vinculación de dispositivos. En el bloque 520, el dispositivo periférico 102 y el dispositivo central 104 se emparejan de modo que se cifre un canal de comunicación inalámbrica establecido entre los mismos y se intercambien una o más claves de seguridad entre el dispositivo periférico 102 y el dispositivo central 104.

Con respecto a los rasgos característicos de seguridad como se describe en esta memoria descriptiva, dichos rasgos característicos pueden incluir rasgos característicos de seguridad fuera de banda (OOB), rasgos

característicos de seguridad MITM y/o rasgos característicos de seguridad de vinculación. Como ejemplo no limitante, el uso de características de seguridad OOB para el emparejamiento permite la autenticación del dispositivo a través del uso de un canal OOB que permite el intercambio de datos de gran tamaño, tales como de hasta 128 bits, a través del canal OOB para potenciar la seguridad de la conexión. Por tanto, el requisito de un rasgo característico de seguridad OOB puede requerir el uso de dicho canal OOB para potenciar la seguridad de la conexión. El canal OOB se puede proteger de ataques MITM y puede ser inmune a interceptaciones de dispositivos inalámbricos no previstos durante la conexión BLE con el dispositivo periférico 102 y el dispositivo central 104.

Los ataques MITM se pueden producir cuando un dispositivo malicioso se hace pasar por uno del dispositivo periférico 102 y el dispositivo central 104, de modo que engaña al otro del dispositivo periférico 102 y el dispositivo central 104 para conectarse con el dispositivo malicioso que puede enrutar y controlar la comunicación entre el dispositivo periférico 102 y el dispositivo central 104. Por tanto, puede parecer que el dispositivo periférico 102 y el dispositivo central 104 están conectados directamente de forma válida sin interferencias, mientras que su conexión, en realidad, se ha visto comprometida. El requisito de rasgos característicos de seguridad MITM requiere protección adicional por parte de los dispositivos contra dichos ataques MITM. Además, un rasgo característico de seguridad de vinculación requiere un intercambio de claves a largo plazo después de la vinculación posterior al emparejamiento del dispositivo periférico 102 y el dispositivo central 104 y el almacenamiento de estas claves a largo plazo para su uso posterior, de modo que el cifrado se pueda iniciar automáticamente sin emparejamiento las posteriores veces que el dispositivo periférico 102 y el dispositivo central 104 se conecten.

En referencia a la fig. 6, se ilustra un procedimiento 604 de emparejamiento positivo basado en escritura de GATT, correspondiente a otro modo de realización de la fase intermedia de emparejamiento positivo 204 de la fig. 2. En particular, la fig. 6 ilustra un procedimiento de emparejamiento positivo basado en escritura de GATT para autenticar un inicio de emparejamiento antes de permitir la presentación de una respuesta de emparejamiento, como se describe con más detalle a continuación.

Al comienzo del procedimiento de emparejamiento positivo basado en escritura de GATT 604, el dispositivo periférico 102 puede poner en marcha un temporizador de escritura de GATT, que se puede establecer para un periodo de tiempo en un intervalo de entre aproximadamente 1 segundo y aproximadamente 5 segundos, tal como aproximadamente 2 segundos. En el bloque 606 se inicia un descubrimiento de servicio de GATT y en el bloque 608 se inicia un descubrimiento de características de GATT. A modo de ejemplo y no como limitación, el dispositivo central 104 inicia un descubrimiento de servicio de GATT con respecto a uno o más servicios de GATT particulares del dispositivo periférico 102 en el bloque 606. En el bloque 608, el dispositivo central 104 inicia además un descubrimiento de servicio de GATT con respecto a una o más características de GATT particulares de los servicios de GATT descubiertos del dispositivo periférico 102 del bloque 606. En el bloque 612, el dispositivo central 104 envía una solicitud de emparejamiento al dispositivo periférico 102 para iniciar el emparejamiento en base a los servicios de GATT descubiertos y las características de GATT de los bloques 606-608 y una comprobación de confirmación de autenticación de emparejamiento del bloque 610, que se describe con más detalle a continuación.

En al menos un modo de realización, las instrucciones legibles por máquina ejecutadas por el uno o más procesadores 1104 pueden provocar que el sistema de emparejamiento de dispositivos 100 use además el dispositivo central 104 para escribir el valor de característica de GATT central en el valor de característica de, por ejemplo, un DIS del dispositivo periférico 102, determine la determinación de coincidencia satisfactoria en base al valor de característica de GATT central que coincide con un valor dispuesto previamente según lo determinado por el dispositivo periférico 102, y determine la determinación de coincidencia no satisfactoria en base al valor de característica de GATT central que no coincide con un valor dispuesto previamente según lo determinado por el dispositivo periférico 102.

Como ejemplo no limitante, en el bloque 610, el dispositivo central 104 escribe un valor de característica central en un valor de característica de un servicio de GATT (tal como el DIS) del dispositivo periférico 102, y el dispositivo periférico 102 confirma la recepción del valor escrito y la escritura para establecer el valor de característica central como el valor de característica de GATT central. En al menos un modo de realización, el dispositivo periférico 102 confirma la recepción de la escritura en al menos un valor de característica de GATT central descubierto del dispositivo periférico 102 por el dispositivo central 104 que da como resultado al menos un valor de característica de GATT central escrito. El valor de característica de GATT central escrito puede incluir o generarse a partir de una lógica que defina al menos uno de los datos predefinidos para escribir en una localización predefinida. Como ejemplo no limitante, el dispositivo central 104 puede recibir un nombre BLE del dispositivo periférico 102 y escribir el mismo valor en un valor de característica de DIS del nombre BLE del dispositivo periférico 102 en el bloque 612. En al menos un modo de realización, el dispositivo periférico 102 puede deshabilitar el temporizador de escritura de GATT después de la confirmación de la escritura del valor de característica de GATT central desde el dispositivo central 104.

En el bloque 616, el procedimiento de emparejamiento positivo basado en escritura de GATT 604 determina, a través de uno o más procesadores 1104, por ejemplo, si el al menos un valor de característica de GATT central escrito del dispositivo periférico 102 coincide con un valor dispuesto previamente. En al menos un modo de

realización, el valor dispuesto previamente lo puede introducir un desarrollador con respecto al GATT del dispositivo periférico 102. De lo contrario, en caso de que el dispositivo central 104 no pueda escribir un valor de característica de GATT central correcto en el dispositivo periférico 102, la autenticación de emparejamiento falla. Tras un fallo de autenticación de emparejamiento, el dispositivo periférico 102 rechaza el emparejamiento y se desconecta del dispositivo central 104 en el bloque 614. Por tanto, un dispositivo que escribe un valor de característica de GATT central incorrecto al dispositivo periférico 102 se puede rechazar para emparejamiento como un dispositivo no previsto y eliminarse como una opción de emparejamiento.

Si se determina una coincidencia en el bloque 616, el procedimiento de emparejamiento positivo basado en escritura de GATT 604 continúa al bloque 618. En el bloque 618, el dispositivo periférico 102 envía una respuesta de emparejamiento al dispositivo central 104. En al menos un modo de realización, la respuesta de emparejamiento es indicativa de un emparejamiento autenticado y no requiere rasgos característicos de seguridad requeridos adicionales para el emparejamiento, tales como de intermediario (MITM) y de vinculación de dispositivos. En el bloque 620, el dispositivo periférico 102 y el dispositivo central 104 se emparejan de modo que se cifre un canal de comunicación inalámbrica establecido entre los mismos y se intercambien una o más claves de seguridad entre el dispositivo periférico 102 y el dispositivo central 104.

Como ejemplo no limitante, las figs. 7 y 10 ilustran respectivamente procedimientos de emparejamiento positivo para autenticar un emparejamiento antes del inicio del emparejamiento como un procedimiento de emparejamiento positivo basado en escritura 704 en la fig. 7 y un procedimiento de emparejamiento positivo basado en autenticación 1004 en la fig. 10, que se describe con más detalle a continuación y que se va a implementar, por ejemplo, por el sistema de emparejamiento de dispositivos 100. Como se describe con más detalle a continuación con respecto a los modos de realización de las figs. 7 y 10, las instrucciones legibles por máquina del sistema de emparejamiento de dispositivos 100 pueden incluir instrucciones para enviar datos de autenticación desde el dispositivo central 104 al dispositivo periférico 102 indicativos de una primera determinación de autenticación; utilizar el dispositivo central 104 para enviar una solicitud de emparejamiento al dispositivo periférico 102 para iniciar el emparejamiento a través del canal de comunicación inalámbrica en base a la primera determinación de autenticación; y determinar una segunda determinación de autenticación antes del emparejamiento de dispositivos en base a si los datos de autenticación indican que la segunda autenticación es satisfactoria o no satisfactoria. Las instrucciones pueden ser además, en respuesta a que la segunda determinación de autenticación sea no satisfactoria, rechazar la solicitud de emparejamiento con el dispositivo periférico 102; en respuesta a que la segunda determinación de autenticación sea satisfactoria, aprobar la solicitud de emparejamiento con el dispositivo periférico 102 y enviar una respuesta de emparejamiento al dispositivo central 104; y emparejar el dispositivo central 104 y el dispositivo periférico 102 en base a la respuesta de emparejamiento para crear el canal de comunicación inalámbrica cifrada.

En referencia a la fig. 7, se ilustra un procedimiento de emparejamiento positivo basado en escritura 704, correspondiente a aún otro modo de realización de la fase intermedia de emparejamiento positivo 204 de la fig. 2. En particular, la fig. 7 ilustra un procedimiento de emparejamiento positivo basado en escritura para autenticar un emparejamiento antes del inicio del emparejamiento, como se describe con más detalle a continuación.

En lugar de escribir en un valor de característica de GATT central específico, tal como un valor de característica de DIS como se establece en el procedimiento de emparejamiento positivo basado en escritura de GATT 604 como se describe anteriormente, el procedimiento de emparejamiento positivo basado en escritura 704 implementa una escritura en una característica específica del dispositivo periférico 102 que puede ser un valor específico para una característica BLE dispuesta previamente del dispositivo periférico. Además, en al menos un modo de realización con respecto a la fig. 7, las instrucciones para enviar datos de autenticación desde el dispositivo central 104 al dispositivo periférico 102 indicativos de una primera determinación de autenticación pueden ser instrucciones para escribir un valor por el dispositivo central 104 en el valor de característica del dispositivo periférico 102, en el que un acontecimiento de escritura es la primera determinación de autenticación. Las instrucciones pueden ser además, como se describe con más detalle a continuación con respecto a la fig. 7, determinar si el valor escrito en el valor de característica del dispositivo periférico 102 coincide con un valor dispuesto previamente para lograr una de una determinación de coincidencia satisfactoria indicativa de que la segunda determinación de autenticación fue satisfactoria y una determinación de coincidencia no satisfactoria indicativa de que la segunda determinación de autenticación fue no satisfactoria.

Al comienzo del procedimiento de emparejamiento positivo basado en escritura 704, el dispositivo periférico 102 puede poner en marcha un temporizador de escritura de GATT, que se puede establecer para un periodo de tiempo en un intervalo de entre aproximadamente 1 segundo y aproximadamente 5 segundos, tal como aproximadamente 2 segundos. En el bloque 705, el dispositivo periférico 102 puede establecer un retraso a través del temporizador de escritura de GATT para una respuesta a la solicitud de emparejamiento. El retraso para una respuesta a la solicitud de emparejamiento establecido en el bloque 705 puede durar un periodo de tiempo en un intervalo de aproximadamente 0,1 a 1 segundo, tal como 0,5 segundos, y se puede establecer en una duración que incluya el periodo de tiempo asociado con la implementación de los bloques 706-709. En el bloque 710, el dispositivo central 104 envía una solicitud de emparejamiento al dispositivo periférico 102 para iniciar el emparejamiento en base a los servicios de GATT descubiertos y las características de GATT y la escritura de los bloques 706-709.

5 En el bloque 706 se inicia un descubrimiento de servicio de GATT y en el bloque 708 se inicia un descubrimiento de características de sub-GATT. A modo de ejemplo y no como limitación, el dispositivo central 104 inicia un descubrimiento de servicio de GATT con respecto a uno o más servicios de GATT particulares del dispositivo periférico 102 en el bloque 706. En el bloque 708, el dispositivo central 104 inicia además un descubrimiento de servicio de GATT con respecto a una o más características de GATT particulares de los servicios de GATT descubiertos del dispositivo periférico 102 del bloque 706.

10 En el bloque 709, el dispositivo central 104 escribe un valor dispuesto previamente en una característica específica del dispositivo periférico 102 y el dispositivo periférico 102 confirma la recepción del valor escrito y la escritura. En al menos un modo de realización, el dispositivo periférico 102 confirma la recepción y la escritura en el valor de característica específico del dispositivo periférico 102 por el dispositivo central 104 que da como resultado al menos un valor de característica de GATT escrito. Como ejemplo no limitante, el dispositivo central 104 escribirá el valor dispuesto previamente en una característica dispuesta previamente del dispositivo periférico 102 según la especificación de BLUETOOTH® Core.

20 En al menos un modo de realización, el dispositivo periférico 102 puede deshabilitar el temporizador de escritura de GATT después de la confirmación de la escritura del valor de característica desde el dispositivo central 104. Dicha acción de escritura ayuda a notificar al dispositivo periférico 102 que el dispositivo central 104 es un dispositivo apropiado y previsto con el que emparejarse. El dispositivo periférico 102 puede rechazar el emparejamiento con el dispositivo central si el dispositivo periférico 102 no confirma la escritura, lo que indica un fallo del dispositivo central 104 al escribir un valor en el dispositivo periférico en el bloque 709.

25 En el bloque 716, el procedimiento de emparejamiento positivo basado en escritura 704 determina, a través de uno o más procesadores 1104, por ejemplo, si el al menos un valor de característica de GATT escrito del dispositivo periférico 102 coincide con un valor dispuesto previamente. En al menos un modo de realización, el valor dispuesto previamente lo puede introducir un desarrollador con respecto al GATT del dispositivo periférico 102. De lo contrario, en caso de el dispositivo central 104 no pueda escribir un valor de característica de GATT correcto en el dispositivo periférico 102, la autenticación de emparejamiento falla. Tras un fallo de autenticación de emparejamiento, el dispositivo periférico 102 rechaza el emparejamiento y se desconecta del dispositivo central 104 en el bloque 714. Por tanto, un dispositivo que escribe un valor de característica de GATT incorrecto al dispositivo periférico 102 se puede rechazar para emparejamiento como un dispositivo no previsto y eliminarse como una opción de emparejamiento.

35 Si se determina una coincidencia en el bloque 716, el procedimiento de emparejamiento positivo basado en escritura 704 continúa al bloque 718. En el bloque 618, el dispositivo periférico 102 envía una respuesta de emparejamiento al dispositivo central 104 indicativa de un emparejamiento autenticado. En el bloque 720, el dispositivo periférico 102 y el dispositivo central 104 se emparejan de modo que se cifre un canal de comunicación inalámbrica establecido entre los mismos y se intercambien una o más claves de seguridad entre el dispositivo periférico 102 y el dispositivo central 104.

45 Como ejemplo no limitante, las figs. 8-9 ilustran respectivamente los procedimientos de emparejamiento positivo basados en el rasgo característico solicitado del modelo de asociación tales como un procedimiento de emparejamiento positivo basado en clave de acceso 804 en la fig. 8 y un procedimiento de emparejamiento positivo basado en fuera de banda (OOB) 904 en la fig. 9, descritos en más detalle a continuación y para que los implemente, por ejemplo, el sistema de emparejamiento de dispositivos 100. Como se describe con más detalle a continuación con respecto a los modos de realización de las figs. 8-9, las instrucciones legibles por máquina del sistema de emparejamiento de dispositivos 100 pueden incluir instrucciones para llevar a cabo, por el dispositivo central, un descubrimiento de características de GATT de un valor de característica del dispositivo periférico 102 a través del canal de comunicación inalámbrica; enviar un rasgo característico solicitado desde el dispositivo central 104 al dispositivo periférico 102 para determinar una determinación de autenticación; determinar la determinación de autenticación antes del emparejamiento de dispositivos en base a si el rasgo característico solicitado recibido por el dispositivo periférico es correcto para lograr una de una determinación satisfactoria y una determinación de coincidencia no satisfactoria; y utilizar el dispositivo central 104 para enviar una solicitud de emparejamiento al dispositivo periférico 102 para iniciar el emparejamiento a través del canal de comunicación inalámbrica en base al descubrimiento de características de GATT del valor de característica (tal como del DIS) del dispositivo periférico 102 y la determinación de autenticación.

60 En respuesta a un hallazgo incorrecto para la determinación de autenticación, la instrucción puede ser rechazar la solicitud de emparejamiento con el dispositivo periférico 102. Las instrucciones pueden comprender además, en respuesta a un hallazgo correcto para la determinación de autenticación como determinación de autenticación, enviar una respuesta de emparejamiento inicial que incluye una solicitud de seguridad para aprobar la solicitud de emparejamiento con el dispositivo periférico 102 y proceder a una segunda determinación de autenticación. Las instrucciones pueden incluir además instrucciones para determinar en la segunda determinación de autenticación si el dispositivo central intercambié claves de seguridad apropiadas con el dispositivo periférico en respuesta a la solicitud de seguridad; en respuesta a un hallazgo negativo para la segunda determinación de autenticación,

rechazar la solicitud de emparejamiento con el dispositivo periférico; y, en respuesta a un hallazgo positivo para la segunda determinación de autenticación, completar el emparejamiento entre el dispositivo periférico y el dispositivo central para crear el canal de comunicación inalámbrica emparejada. En modos de realización, el rasgo característico solicitado es un valor predefinido de un modelo de asociación, cuyos ejemplos no limitantes se describen a continuación con más detalle. Las instrucciones pueden ser además determinar la determinación de autenticación antes del emparejamiento de dispositivos en base a si el rasgo característico solicitado recibido por el dispositivo periférico 102 es correcto para lograr una de una determinación satisfactoria y una determinación de coincidencia no satisfactoria comprenden instrucciones para determinar si el valor predefinido del modelo de asociación recibido por el dispositivo periférico 102 coincide con un valor esperado del modelo de asociación.

En referencia a la fig. 8, se ilustra un procedimiento de modelo de asociación tal como un procedimiento de emparejamiento positivo basado en clave de acceso 804, correspondiente a aún otro modo de realización de la fase intermedia de emparejamiento positivo 204 de la fig. 2. En particular, la fig. 8 ilustra un procedimiento de emparejamiento positivo basado en clave de acceso para autenticar un inicio de emparejamiento antes de permitir la presentación de una respuesta de emparejamiento y en el que el rasgo característico solicitado es una clave de acceso predefinida, como se describe con más detalle a continuación.

En un procedimiento de usuario manual, el dispositivo periférico 102 generaría un pin aleatorio de 6 dígitos que se mostraría para que el usuario lo tome e introduzca como un código de emparejamiento para confirmar el emparejamiento en una pantalla de visualización del dispositivo central 104. Dicho procedimiento de hacer que los usuarios finales introduzcan un código de emparejamiento para autenticar el emparejamiento puede dar como resultado problemas tales como errores de usuario y tiempo adicional para completar el emparejamiento.

El procedimiento de emparejamiento positivo basado en clave de acceso 804 permite una autenticación automatizada a través de un enfoque de código en el que se usa un código fijo para el código de clave de acceso que el dispositivo central 104 enviará al dispositivo periférico 102, como se describe con más detalle a continuación. Como ejemplo no limitante, el dispositivo periférico 102 solicitará la clave de acceso BLE y el dispositivo central 104 enviará el código fijo como un código estático de 6 dígitos para confirmar el emparejamiento. Por tanto, un usuario final no necesitará introducir manualmente la clave de acceso, y el código de clave de acceso sería estático para todos los dichos emparejamientos entre el dispositivo central 104 y el dispositivo periférico 102. De forma alternativa, la clave de acceso puede ser un valor dinámico en base a la información intercambiada entre el dispositivo central 104 y el dispositivo periférico 102 cuando están conectados, tal como un número de serie del dispositivo periférico 102 determinado a partir de un descubrimiento de características de GATT como se describe a continuación, por ejemplo. La lógica del dispositivo periférico 102, tal como la lógica implementada a través del uno o más procesadores 1104, puede definir además reglas para determinar una generación automatizada de código para que el dispositivo central 104 lo envíe al dispositivo periférico 102 como valor de clave de acceso predefinido.

En el bloque 806 se inicia un descubrimiento de servicio de GATT y en el bloque 808 se inicia un descubrimiento de características de GATT de subconjunto. A modo de ejemplo y no como limitación, el dispositivo central 104 inicia un descubrimiento de servicio de GATT con respecto a uno o más servicios de GATT particulares del dispositivo periférico 102 en el bloque 806. En el bloque 808, el dispositivo central 104 inicia además un descubrimiento de características de GATT con respecto a una o más características de GATT particulares de los servicios de GATT descubiertos del dispositivo periférico 102 del bloque 806. En el bloque 813, el dispositivo central 104 envía una solicitud de emparejamiento al dispositivo periférico 102 para iniciar el emparejamiento en base a los servicios de GATT descubiertos y las características de GATT de los bloques 806-808 y una comprobación de confirmación de autenticación de emparejamiento del bloque 810.

En el bloque 810, el dispositivo central 104 envía una clave de acceso predefinida para autenticar el emparejamiento al dispositivo periférico 102. El dispositivo central 104 también debería enviar una respuesta de seguridad a la solicitud de seguridad para el uno o más rasgos característicos de seguridad requeridos adicionales, tal como la presentación del uno o más rasgos característicos de seguridad requeridos adicionales.

En el bloque 816, el procedimiento de emparejamiento positivo basado en clave de acceso 804 determina, a través de uno o más procesadores 1104, por ejemplo, si la clave de acceso predefinida recibida por el dispositivo periférico 102 coincide con un valor dispuesto previamente. En al menos un modo de realización, el valor dispuesto previamente lo puede introducir un desarrollador con respecto al dispositivo periférico 102. De lo contrario, en caso de que el dispositivo central 104 no pueda enviar una clave de acceso, o no pueda enviar una clave de acceso correcta, al dispositivo periférico 102, la autenticación de emparejamiento falla. Tras un fallo de autenticación de emparejamiento, el dispositivo periférico 102 rechaza el emparejamiento y se desconecta del dispositivo central 104 en el bloque 814. Por tanto, un dispositivo que envía una clave de acceso incorrecta o que no puede enviar una clave de acceso al dispositivo periférico 102 se puede rechazar para emparejamiento como un dispositivo no previsto y eliminarse como una opción de emparejamiento.

Si se determina una coincidencia en el bloque 816, el procedimiento de emparejamiento positivo basado en clave de acceso 804 continúa al bloque 818. En el bloque 818, el dispositivo periférico 102 envía una respuesta de

emparejamiento al dispositivo central 104 junto con una solicitud de seguridad para uno o más rasgos característicos de seguridad requeridos adicionales, tales como para MITM y vinculación. En el bloque 820, el dispositivo periférico 102 y el dispositivo central 104 se emparejan de modo que se cifre un canal de comunicación inalámbrica establecido entre los mismos y se intercambien una o más claves de seguridad entre el dispositivo periférico 102 y el dispositivo central 104. En el bloque 822, el procedimiento de emparejamiento positivo basado en clave de acceso 804 determina, a través de uno o más procesadores 1104, por ejemplo, si el dispositivo central 104 intercambió claves de seguridad apropiadas con el dispositivo periférico 102. De lo contrario, el dispositivo periférico 102 rechaza el emparejamiento en el bloque 814. En al menos un modo de realización, una pantalla de visualización del dispositivo periférico 102 y/o el dispositivo central 104 puede mostrar un mensaje de rechazo, tal como "emparejamiento rechazado" o "bomba no encontrada", si el procedimiento de emparejamiento positivo basado en clave de acceso 804 determina que el dispositivo central 104 no intercambió claves de seguridad apropiadas con el dispositivo periférico 102.

Si es así, el emparejamiento se completa entre el dispositivo periférico 102 y el dispositivo central 104 en el bloque 824. Como ejemplo no limitante, en el bloque 813, el dispositivo central 104 debería haber enviado la respuesta de seguridad a la solicitud de seguridad para el uno o más rasgos característicos de seguridad requeridos adicionales, tales como MITM y vinculación. Si se envió la respuesta de seguridad apropiada, el emparejamiento se completa en el bloque 824. De otro modo, el emparejamiento se rechaza en el bloque 814.

En referencia a la fig. 9, se ilustra un procedimiento de emparejamiento positivo basado en OOB 904, correspondiente a aún otro modo de realización de la fase intermedia de emparejamiento positivo 204 de la fig. 2. En particular, la fig. 9 ilustra un procedimiento de emparejamiento positivo basado en OOB para autenticar un inicio de emparejamiento antes de recibir una respuesta de emparejamiento y en el que el rasgo característico solicitado es una matriz de datos OOB predefinida, como se describe con más detalle a continuación.

Con el procedimiento de emparejamiento positivo basado en OOB 904, el dispositivo central 104 y el dispositivo periférico 102 podrían usar datos OOB como un mecanismo para que el dispositivo central 104 se identifique correctamente con el dispositivo periférico 102, como se describe con más detalle a continuación. Como ejemplo no limitante, el dispositivo central 104 enviaría una solicitud de emparejamiento e intentaría emparejarse con el dispositivo periférico 102. Por su parte, el dispositivo periférico 102 respondería con una solicitud de seguridad en la que se requieren rasgos característicos de seguridad OOB, MITM y de vinculación. A continuación, se requeriría que el dispositivo central 104 respondiera a la solicitud de seguridad con una respuesta de seguridad que incluya al menos una matriz de datos OOB predefinida, como se describe con más detalle a continuación, para autenticar el emparejamiento.

Con respecto al procedimiento de emparejamiento positivo basado en OOB 904, en el bloque 906 se inicia un descubrimiento de servicio de GATT y en el bloque 908 se inicia un descubrimiento de características de GATT. A modo de ejemplo y no como limitación, el dispositivo central 104 inicia un descubrimiento de servicio de GATT con respecto a uno o más servicios de GATT particulares del dispositivo periférico 102 en el bloque 906. En el bloque 908, el dispositivo central 104 inicia además un descubrimiento de servicio de GATT con respecto a una o más características de GATT particulares de los servicios de GATT descubiertos del dispositivo periférico 102 del bloque 906. En el bloque 912, el dispositivo central 104 envía una solicitud de emparejamiento al dispositivo periférico 102 para iniciar el emparejamiento en base a los servicios de GATT descubiertos y las características de GATT de los bloques 906-908 y una comprobación de confirmación de autenticación de emparejamiento del bloque 910.

En el bloque 910, el dispositivo central 104 envía una matriz de datos fuera de banda (OOB) predefinida para autenticar el emparejamiento al dispositivo periférico 102. El dispositivo central 104 también debería enviar una respuesta de seguridad a la solicitud de seguridad adicional para el uno o más rasgos característicos de seguridad requeridos adicionales, tal como la presentación del uno o más rasgos característicos de seguridad requeridos adicionales.

En el bloque 916, el procedimiento de emparejamiento positivo basado en OOB 904 determina, a través de uno o más procesadores 1104, por ejemplo, si la matriz de datos OOB predefinida recibida por el dispositivo periférico 102 coincide con una matriz de datos OOB esperada y es correcta. En al menos un modo de realización, la matriz de datos OOB esperada la puede introducir un desarrollador con respecto al dispositivo periférico 102. De lo contrario, en caso de que el dispositivo central 104 no pueda enviar una matriz de datos OOB predefinida, o no pueda enviar una matriz de datos OOB predefinida correcta, al dispositivo periférico 102, la autenticación de emparejamiento falla. Tras un fallo de autenticación de emparejamiento, el dispositivo periférico 102 rechaza el emparejamiento y se desconecta del dispositivo central 104 en el bloque 914. Por tanto, un dispositivo que envía una matriz de datos OOB predefinida incorrecta o que no puede enviar una matriz de datos OOB predefinida al dispositivo periférico 102 se puede rechazar para emparejamiento como un dispositivo no previsto y eliminarse como una opción de emparejamiento.

Si se determina una presentación correcta de la matriz de datos OOB predefinida en el bloque 916, el procedimiento de emparejamiento positivo basado en OOB 904 continúa al bloque 918. En el bloque 918, el

dispositivo periférico 102 envía una respuesta de emparejamiento al dispositivo central 104 junto con una solicitud de seguridad para un rasgo característico de seguridad OOB, así como para uno o más rasgos característicos de seguridad requeridos adicionales, tales como para MITM y vinculación.

5 En el bloque 920, el dispositivo periférico 102 y el dispositivo central 104 se emparejan de modo que se cifre un canal de comunicación inalámbrica establecido entre los mismos y se intercambien una o más claves de seguridad entre el dispositivo periférico 102 y el dispositivo central 104.

10 En el bloque 922, el procedimiento de emparejamiento positivo basado en OOB 904 determina, a través de uno o más procesadores 1104, por ejemplo, si el dispositivo central 104 intercambió claves de seguridad apropiadas con el dispositivo periférico 102. De lo contrario, el dispositivo periférico 102 rechaza el emparejamiento en el bloque 914. Si es así, el emparejamiento se completa entre el dispositivo periférico 102 y el dispositivo central 104 en el bloque 924. Como ejemplo no limitante, en el bloque 912, el dispositivo central 104 debería haber enviado la respuesta de seguridad a la solicitud de seguridad para el uno o más rasgos característicos de seguridad requeridos adicionales, tales como MITM y vinculación además de la matriz de datos OOB predefinida. Si se envió la respuesta de seguridad apropiada, el emparejamiento se completa en el bloque 824. De otro modo, el emparejamiento se rechaza en el bloque 914.

20 En referencia a la fig. 10, se ilustra un procedimiento de emparejamiento positivo basado en autenticación 1004, correspondiente a otro modo de realización de la fase intermedia de emparejamiento positivo 204 de la fig. 2. En particular, la fig. 10 ilustra un procedimiento de emparejamiento positivo basado en autenticación para autenticar un emparejamiento antes del inicio del emparejamiento, como se describe con más detalle a continuación.

25 En lugar de leer o escribir en un valor de característica específico como se establece en los procedimientos de emparejamiento positivo 504-704, o de enviar una clave de acceso o matriz de datos OOB como se establece en los procedimientos de emparejamiento positivo 804-904 como se describe anteriormente, el procedimiento de emparejamiento positivo basado en autenticación 1004 implementa una autenticación de dispositivo tal como un intercambio de claves de dispositivo. En al menos un modo de realización, el intercambio de claves de dispositivo incluye datos de autenticación de dispositivo como una clave de dispositivo indicativa de un dispositivo autenticado para permitir una autenticación por el dispositivo periférico 102 del dispositivo central 104 como dispositivo autenticado, aceptable y deseado con el cual emparejarse antes de que el dispositivo central 104 inicie el emparejamiento con el dispositivo periférico 102. Además, en al menos un modo de realización con respecto a la fig. 10, instrucciones para enviar datos de autenticación del dispositivo en respuesta a una solicitud de datos de autenticación del dispositivo desde el dispositivo periférico.

35 Al comienzo del procedimiento de emparejamiento positivo basado en autenticación 1004, el dispositivo periférico 102 puede poner en marcha un temporizador de autenticación establecido para un periodo de tiempo en un intervalo de aproximadamente 1 segundo a aproximadamente 5 segundos, tal como durante 2 segundos. En el bloque 1005, el dispositivo periférico 102 puede establecer un retraso para una respuesta a la solicitud de emparejamiento. El retraso para una respuesta a la solicitud de emparejamiento establecido en el bloque 1005 puede durar un periodo de tiempo en un intervalo de aproximadamente 0,1 a 1 segundo, tal como 0,5 segundos, y se puede establecer en una duración que incluya el periodo de tiempo asociado con la implementación de los bloques 1006-1008.

45 En el bloque 1006 se inicia un descubrimiento de servicio de GATT y en el bloque 1008 se inicia un descubrimiento de características de GATT. A modo de ejemplo y no como limitación, el dispositivo central 104 inicia un descubrimiento de servicio de GATT con respecto a uno o más servicios de GATT particulares del dispositivo periférico 102 en el bloque 1006. En el bloque 1008, el dispositivo central 104 inicia además un descubrimiento de características de GATT con respecto a una o más características de GATT particulares de los servicios de GATT descubiertos del dispositivo periférico 102 del bloque 1006. El tiempo para implementar los bloques 1005 a 1008 puede durar entre alrededor de 0,1 segundos a alrededor de 1 segundo, tal como alrededor de 0,5 segundos.

55 En los bloques 1010-1012, un intercambio de claves de dispositivo permite una autenticación por el dispositivo periférico 102 del dispositivo central 104 como dispositivo deseado y aceptable con el cual emparejarse antes de que el dispositivo central 104 inicie el emparejamiento con el dispositivo periférico 102 en el bloque 1013. Como ejemplo no limitante, en el bloque 1010, el dispositivo periférico 102 envía una solicitud al dispositivo central 104 de datos de autenticación del dispositivo. En el bloque 1012, el dispositivo central 104 envía los datos de autenticación del dispositivo al dispositivo periférico 102. De forma alternativa, el dispositivo central 104 puede enviar directamente datos de autenticación del dispositivo al dispositivo periférico 102 sin responder a una solicitud de dichos datos. Después del bloque 1012, el dispositivo periférico 102 puede deshabilitar el temporizador de autenticación.

65 En al menos un modo de realización, el dispositivo periférico 102 puede deshabilitar el temporizador de autenticación después de la confirmación del dispositivo central 104 que envía datos de autenticación del dispositivo al dispositivo periférico 102 en el bloque 1012. Dicha presentación de datos de autenticación del bloque 1012 ayuda a notificar al dispositivo periférico 102 que el dispositivo central 104 es un dispositivo apropiado y

previsto con el que emparejarse. El dispositivo periférico 102 puede rechazar el emparejamiento con el dispositivo central 104 si el dispositivo periférico 102 no confirma la presentación de datos de autenticación del bloque 1012, lo que indica un fallo del dispositivo central 104 al proporcionar los datos de autenticación al dispositivo periférico en el bloque 1012.

5

En el bloque 1013, el dispositivo central 104 envía una solicitud de emparejamiento al dispositivo periférico 102 para iniciar el emparejamiento en base a los servicios de GATT descubiertos y las características de GATT y la autenticación del dispositivo de los bloques 1006-1012.

10

En el bloque 1016, el procedimiento de emparejamiento positivo basado en autenticación 1004 determina, a través de uno o más procesadores 1104, por ejemplo, si los datos de autenticación del dispositivo enviados al dispositivo periférico 102 en el bloque 1012 por el dispositivo central 104 dan como resultado una autenticación satisfactoria del dispositivo, tal como cuando los datos de autenticación del dispositivo presentados en el bloque 1012 coinciden con los datos de autenticación del dispositivo dispuestos previamente según lo determinado por el dispositivo periférico 102. En al menos un modo de realización, los datos de autenticación del dispositivo del valor dispuesto previamente o las reglas con respecto a una autenticación satisfactoria del dispositivo los puede introducir un desarrollador con respecto al dispositivo periférico 102. De lo contrario, en caso de que el dispositivo central 104 no pueda proporcionar datos de autenticación del dispositivo correctos en el bloque 1012 para dar como resultado una autenticación satisfactoria del dispositivo en el bloque 1016, la autenticación de emparejamiento falla. Tras un fallo de autenticación de emparejamiento, el dispositivo periférico 102 rechaza el emparejamiento y se desconecta del dispositivo central 104 en el bloque 1014. Por tanto, un dispositivo que no presenta datos de autenticación del dispositivo en el bloque 1012 o que no presenta datos de autenticación del dispositivo correctos para dar como resultado una autenticación satisfactoria del dispositivo en el bloque 1016 se puede rechazar para emparejamiento como dispositivo no previsto y eliminarse como opción de emparejamiento.

15

20

25

Si se determina una coincidencia de autenticación satisfactoria de dispositivo en el bloque 1016, el procedimiento de emparejamiento positivo basado en autenticación 1004 continúa al bloque 1018. En el bloque 1018, el dispositivo periférico 102 envía una respuesta de emparejamiento al dispositivo central 104 indicativa de un emparejamiento autenticado. En el bloque 1020, el dispositivo periférico 102 y el dispositivo central 104 se emparejan de modo que se cifre un canal de comunicación inalámbrica establecido entre los mismos y se intercambien una o más claves de seguridad entre el dispositivo periférico 102 y el dispositivo central 104.

30

35

En referencia a la fig. 11, se ilustra un sistema 1100 para implementar un procedimiento informático y basado en programa informático para utilizar el sistema de emparejamiento de dispositivos como fases asociadas, como se muestra en las figs. 1-10, y se puede implementar junto con el uso de una interfaz gráfica de usuario (GUI) 1124 que es accesible en un puesto de trabajo de usuario, por ejemplo, un dispositivo informático y/o en los dispositivos periféricos y centrales 102, 104, que pueden ser dispositivos médicos, por ejemplo. El sistema 1100 incluye una ruta de comunicación 1102, uno o más procesadores 1104, uno o más componentes de memoria 1106, un componente de perfil 1112, un almacenamiento o base de datos 1114, un equipo informático de interfaz de red 1118, un servidor 1120, una red 1122, dispositivos 102, 104 y al menos una GUI 1124. Los diversos componentes del sistema 1100 y la interacción de los mismos se describirán en detalle a continuación.

40

45

Si bien solo se ilustra un servidor de aplicaciones 1120 y una GUI 1124 que pueden formar parte de un puesto de trabajo, el sistema 1100 puede incluir múltiples puestos de trabajo y servidores de aplicaciones que contienen una o más aplicaciones que se pueden localizar en localizaciones geográficamente diversas en una pluralidad de sitios industriales. En algunos modos de realización, el sistema 1100 se implementa usando una red de área amplia (WAN) o una red 1122, tal como una intranet o Internet, u otra red de comunicación alámbrica o inalámbrica, que puede incluir una configuración de red basada en informática en la nube (por ejemplo, "la nube"). El ordenador del puesto de trabajo puede incluir sistemas digitales y otros dispositivos que permiten la conexión a y la navegación por la red. Son posibles otras variaciones del sistema 1100 que permiten la comunicación entre diversos componentes geográficamente diversos. Las líneas representadas en la fig. 11 indican comunicación en lugar de conexiones físicas entre los diversos componentes.

50

55

Como se indica anteriormente, el sistema 1100 incluye la ruta de comunicación 1102. La ruta de comunicación 1102 se puede formar a partir de cualquier medio que pueda transmitir una señal tal como, por ejemplo, cables conductores, pistas conductoras, guías de ondas ópticas o similares, o de una combinación de medios que puedan transmitir señales. La ruta de comunicación 1102 acopla de forma comunicativa los diversos componentes del sistema 1100. Como se usa en el presente documento, el término "acoplado de forma comunicativa" significa que los componentes acoplados pueden intercambiar señales de datos entre sí, tal como, por ejemplo, señales eléctricas por medio de un medio conductor, señales electromagnéticas por medio del aire, señales ópticas por medio de guías de ondas ópticas y similares.

60

65

Como se indica anteriormente, el sistema 1100 incluye el uno o más procesadores 1104. El uno o más procesadores 1104 pueden ser cualquier dispositivo que pueda ejecutar instrucciones legibles por máquina. En consecuencia, el uno o más procesadores 1104 pueden ser un controlador, un circuito integrado, un microchip, un ordenador o cualquier otro dispositivo informático. El uno o más procesadores 1104 se acoplan de forma

comunicativa a los otros componentes del sistema 1100 mediante la ruta de comunicación 1102. En consecuencia, la ruta de comunicación 1102 puede acoplar de forma comunicativa cualquier número de procesadores entre sí, y permitir que los módulos acoplados a la ruta de comunicación 1102 funcionen en un entorno informático distribuido. Específicamente, cada uno de los módulos puede funcionar como un nodo que puede enviar y/o recibir datos. El uno o más procesadores 1104 pueden procesar las señales de entrada recibidas desde los módulos de sistema y/o extraer información de dichas señales.

Como se indica anteriormente, el sistema 1100 incluye el uno o más componentes de memoria 1106 que se acoplan a la ruta de comunicación 1102 y se acoplan de forma comunicativa al procesador 1104.

El uno o más componentes de memoria 1106 pueden ser un medio no transitorio legible por ordenador o una memoria no transitoria legible por ordenador y se pueden configurar como un medio no volátil legible por ordenador. El uno o más componentes de memoria 1106 pueden comprender RAM, ROM, memorias *flash*, discos duros o cualquier dispositivo que pueda almacenar instrucciones legibles por máquina de modo que el uno o más procesadores 1104 puedan acceder a y ejecutar las instrucciones legibles por máquina. Las instrucciones legibles por máquina pueden comprender lógica o algoritmos escritos en cualquier lenguaje de programación tal como, por ejemplo, lenguaje de máquina que se puede ejecutar directamente por el procesador, o lenguaje ensamblador, programación orientada a objetos (POO), lenguajes de secuencias de comandos, microcódigo, etc., que se puede compilar o ensamblar en instrucciones legibles por máquina y almacenarse en el uno o más componentes de memoria 1106. De forma alternativa, las instrucciones legibles por máquina se pueden escribir en un lenguaje de descripción de equipo informático (HDL), tal como lógica implementada por medio de una configuración de matriz de puertas programables por campo (FPGA) o un circuito integrado específico de la aplicación (ASIC), o sus equivalentes. En consecuencia, los procedimientos descritos en el presente documento se pueden implementar en cualquier lenguaje de programación informático convencional, como elementos de equipo informático preprogramados o como una combinación de componentes de equipo informático y programa informático. En modos de realización, el sistema 1100 puede incluir el uno o más procesadores 1104 acoplados de forma comunicativa al uno o más componentes de memoria 1106 que almacenan instrucciones que, cuando las ejecutan el uno o más procesadores 1104, provocan que el procesador realice una o más funciones como se describe en el presente documento.

Todavía en referencia a la fig. 11, como se indica anteriormente, el sistema 1100 comprende el monitor tal como una GUI 1124 en una pantalla de un dispositivo informático para proporcionar una salida visual tal como, por ejemplo, información, informes gráficos, mensajes o una combinación de los mismos. El dispositivo informático, tal como los dispositivos 102, 104, puede incluir uno o más dispositivos informáticos a través de plataformas, o se puede acoplar de forma comunicativa a dispositivos a través de plataformas, tales como dispositivos móviles inteligentes que incluyen teléfonos inteligentes, tabletas, ordenadores portátiles y/o similares o dispositivos médicos tales como medidores de glucemia, bombas de insulina, monitores continuos de glucosa y similares. El monitor en la pantalla del dispositivo informático se acopla a la ruta de comunicación 1102 y se acopla de forma comunicativa al uno o más procesadores 1104. En consecuencia, la ruta de comunicación 1102 acopla de forma comunicativa el monitor a otros módulos del sistema 1100. El monitor puede incluir cualquier medio que pueda transmitir una salida óptica tal como, por ejemplo, un tubo de rayos catódicos, diodos emisores de luz, un monitor de cristal líquido, un monitor de plasma o similares. Adicionalmente, cabe señalar que el monitor o el dispositivo informático tal como el dispositivo 102, 104 puede incluir al menos uno del uno o más procesadores 1104 y el uno o más componentes de memoria 1106. Si bien el sistema 1100 se ilustra como un sistema único e integrado en la fig. 11, en otros modos de realización, los sistemas pueden ser sistemas independientes.

El sistema 1100 comprende el componente de perfil 1112 que, en al menos un modo de realización, es representativo de la arquitectura BLE con respecto al GATT, cada uno del dispositivo periférico 102 y el dispositivo central 104 como se describe en el presente documento. El componente de perfil 1112 se acopla a la ruta de comunicación 1102 y se acopla de forma comunicativa al uno o más procesadores 1104. Como se describirá en más detalle a continuación, el uno o más procesadores 1104 pueden procesar las señales de entrada recibidas desde los módulos de sistema y/o extraer información de dichas señales.

El sistema 1100 incluye el equipo informático de interfaz de red 1118 para acoplar de forma comunicativa el sistema 1100 a una red informática tal como la red 1122. El equipo informático de interfaz de red 1118 se acopla a la ruta de comunicación 1102 de modo que la ruta de comunicación 1102 acople de forma comunicativa el equipo informático de interfaz de red 1118 a otros módulos del sistema 1100. El equipo informático de interfaz de red 1118 puede ser cualquier dispositivo que pueda transmitir y/o recibir datos por medio de una red inalámbrica. En consecuencia, el equipo informático de interfaz de red 1118 puede incluir un transceptor de comunicación para enviar y/o recibir datos de acuerdo con cualquier norma de comunicación inalámbrica. Por ejemplo, el equipo informático de interfaz de red 1118 puede incluir un conjunto de chips (por ejemplo, antena, procesadores, instrucciones legibles por máquina, etc.) para comunicarse por medio de redes informáticas alámbricas y/o inalámbricas tales como, por ejemplo, fidelidad inalámbrica (Wi-Fi), WiMax, BLUETOOTH®, IrDA, USB inalámbrico, Z-Wave, ZigBee o similares.

En referencia todavía a la fig. 11, los datos de diversas aplicaciones que se ejecutan en dispositivos informáticos

tales como los dispositivos 102, 104 se pueden proporcionar desde los dispositivos 102, 104 al sistema 1100 por medio del equipo informático de interfaz de red 1118. El dispositivo informático puede ser cualquier dispositivo que tenga equipo informático (por ejemplo, conjuntos de chips, procesadores, memoria, etc.) para acoplarse de forma comunicativa al equipo informático de interfaz de red 1118 y a una red 1122. Específicamente, el dispositivo informático puede incluir un dispositivo de entrada que tiene una antena para comunicarse a través de una o más de las redes informáticas inalámbricas descritas anteriormente.

La red 1122 puede incluir cualquier red alámbrica y/o inalámbrica tal como, por ejemplo, redes de área amplia, redes de área metropolitana, Internet, una Intranet, la nube, redes satelitales o similares. En consecuencia, el ordenador 1104 puede utilizar la red 1122 como punto de acceso inalámbrico para acceder a uno o más servidores (por ejemplo, un servidor 1120). El servidor 1120 y cualquier servidor adicional incluyen en general procesadores, memoria y conjunto de chips para suministrar recursos por medio de la red 1122. Los recursos pueden incluir proporcionar, por ejemplo, procesamiento, almacenamiento, programa informático e información desde el servidor 1120 al sistema 1100 por medio de la red 1122. Adicionalmente, cabe señalar que el servidor 1120 y cualquier servidor adicional pueden compartir recursos entre sí a través de la red 1122 tal como, por ejemplo, a través de la porción alámbrica de la red, la porción inalámbrica de la red o combinaciones de las mismas.

En un ejemplo que no forma parte de la invención como se reivindica, un sistema de emparejamiento de dispositivos puede incluir un dispositivo periférico, un dispositivo central, el sistema de emparejamiento de dispositivos configurado para emparejar el dispositivo periférico y el dispositivo central para establecer un canal de comunicación inalámbrica emparejada entre los mismos, uno o más procesadores, uno o más componentes de memoria acoplados de forma comunicativa al uno o más procesadores, e instrucciones legibles por máquina almacenadas en el uno o más componentes de memoria que provocan que el sistema de emparejamiento de dispositivos realice al menos lo siguiente cuando las ejecuta el uno o más procesadores: establecer una conexión a través de un canal de comunicación inalámbrica entre el dispositivo periférico y el dispositivo central; llevar a cabo, por el dispositivo central, un descubrimiento de características de GATT de un valor de característica de GATT de un servicio de GATT del dispositivo periférico a través del canal de comunicación inalámbrica; determinar una determinación de autenticación antes del emparejamiento de dispositivos en base a la determinación de un valor de característica de GATT central para lograr una de una determinación de coincidencia satisfactoria y una determinación de coincidencia no satisfactoria; utilizar el dispositivo central para enviar una solicitud de emparejamiento al dispositivo periférico para iniciar el emparejamiento a través del canal de comunicación inalámbrica en base al descubrimiento de características de GATT del valor de característica de GATT del servicio de GATT del dispositivo periférico; en respuesta a la determinación de coincidencia no satisfactoria como determinación de autenticación, rechazar la solicitud de emparejamiento con el dispositivo periférico; en respuesta a la determinación de coincidencia satisfactoria como determinación de autenticación, aprobar la solicitud de emparejamiento con el dispositivo periférico y enviar una respuesta de emparejamiento al dispositivo central; y emparejar el dispositivo central y el dispositivo periférico en base a la respuesta de emparejamiento para crear el canal de comunicación inalámbrica emparejada.

En el ejemplo, el valor de característica de GATT del servicio de GATT del dispositivo periférico puede comprender un valor de característica de un servicio de información del dispositivo (DIS) del dispositivo periférico. En un ejemplo, las instrucciones para determinar una determinación de autenticación antes del emparejamiento de dispositivos en base a la determinación de un valor de característica de GATT central del dispositivo central para lograr una de una determinación de coincidencia satisfactoria y una determinación de coincidencia no satisfactoria pueden comprender instrucciones para: llevar a cabo, por el dispositivo periférico, un descubrimiento de características de GATT de un valor de característica central del dispositivo central a través del canal de comunicación inalámbrica; leer el valor de característica central por el dispositivo periférico para establecer el valor de característica central como el valor de característica de GATT central; determinar la determinación de coincidencia satisfactoria en base al valor de característica de GATT central que coincide con un valor dispuesto previamente según lo determinado por el dispositivo periférico; y determinar la determinación de coincidencia no satisfactoria en base al valor de característica de GATT central que no coincide con un valor dispuesto previamente según lo determinado por el dispositivo periférico.

El valor de característica central es uno de un valor de característica de DIS o un identificador único universal (UUID).

En un ejemplo, las instrucciones para determinar una determinación de autenticación antes del emparejamiento de dispositivos en base a la determinación de un valor de característica de GATT central para lograr una de una determinación de coincidencia satisfactoria y una determinación de coincidencia no satisfactoria pueden comprender instrucciones para: usar el dispositivo central para escribir el un valor de característica central en un valor de característica del dispositivo periférico para establecer el valor de característica central como el valor de característica de GATT central; determinar la determinación de coincidencia satisfactoria en base al valor de característica de GATT central que coincide con un valor dispuesto previamente según lo determinado por el dispositivo periférico; y determinar la determinación de coincidencia no satisfactoria en base al valor de característica de GATT central que no coincide con un valor dispuesto previamente según lo determinado por el dispositivo periférico.

En un ejemplo, el valor de característica de GATT central puede comprender un número de serie del dispositivo periférico presentado por el dispositivo periférico al dispositivo central.

5 En un ejemplo, el sistema de emparejamiento de dispositivos puede comprender instrucciones para transmitir el número de serie del dispositivo periférico desde el dispositivo periférico al dispositivo central a través del canal de comunicación inalámbrica.

10 En un ejemplo, las instrucciones pueden comprender además instrucciones para intercambiar uno o más rasgos característicos de clave de seguridad entre el dispositivo central y el dispositivo periférico antes de emparejar el dispositivo central y el dispositivo periférico.

15 En un ejemplo, el sistema de emparejamiento de dispositivos puede comprender además instrucciones para vincular el dispositivo periférico y el dispositivo central de modo que, después de emparejar el dispositivo periférico y el dispositivo central, almacenen el uno o más rasgos característicos de clave de seguridad que se intercambian.

En un ejemplo, el sistema de emparejamiento de dispositivos puede comprender además instrucciones para desconectar el dispositivo periférico y el dispositivo central después de la vinculación.

20 En un ejemplo, las instrucciones para establecer una conexión a través de un canal de comunicación inalámbrica entre el dispositivo periférico y el dispositivo central pueden comprender además instrucciones para colocar cada uno del dispositivo periférico y el dispositivo central en un modo de emparejamiento.

25 En un ejemplo, el sistema de emparejamiento de dispositivos puede comprender además instrucciones para: poner en marcha un temporizador de autenticación al comienzo del descubrimiento de características de GATT; deshabilitar el temporizador de autenticación en respuesta a la determinación de coincidencia satisfactoria como determinación de autenticación; y mostrar una confirmación de emparejamiento en una pantalla de visualización respectiva de cada uno del dispositivo central y el dispositivo periférico después de emparejar el dispositivo central y el dispositivo periférico en base a la respuesta de emparejamiento.

30 En un ejemplo que no forma parte de la invención como se reivindica, un sistema de emparejamiento de dispositivos puede incluir un dispositivo periférico, un dispositivo central, el sistema de emparejamiento de dispositivos configurado para emparejar el dispositivo periférico y el dispositivo central para establecer un canal de comunicación inalámbrica emparejada entre los mismos, uno o más procesadores, uno o más componentes de memoria acoplados de forma comunicativa al uno o más procesadores, e instrucciones legibles por máquina almacenadas en el uno o más componentes de memoria que provocan que el sistema de emparejamiento de dispositivos realice al menos lo siguiente cuando las ejecuta el uno o más procesadores: establecer una conexión a través de un canal de comunicación inalámbrica entre el dispositivo periférico y el dispositivo central; llevar a cabo, por el dispositivo central, un descubrimiento de características de GATT de un valor de característica del dispositivo periférico a través del canal de comunicación inalámbrica; enviar un rasgo característico solicitado desde el dispositivo central al dispositivo periférico para determinar una determinación de autenticación; determinar la determinación de autenticación antes del emparejamiento de dispositivos en base a si el rasgo característico solicitado recibido por el dispositivo periférico es correcto para lograr una de una determinación satisfactoria y una determinación de coincidencia no satisfactoria; utilizar el dispositivo central para enviar una solicitud de emparejamiento al dispositivo periférico para iniciar el emparejamiento a través del canal de comunicación inalámbrica en base al descubrimiento de características de GATT del dispositivo periférico y la determinación de autenticación; en respuesta a un hallazgo incorrecto para la determinación de autenticación, rechazar la solicitud de emparejamiento con el dispositivo periférico; en respuesta a un hallazgo correcto para la determinación de autenticación, enviar una respuesta de emparejamiento inicial por parte del dispositivo periférico que incluye una solicitud de seguridad y proceder a una segunda determinación de autenticación; determinar, en la segunda determinación de autenticación, si el dispositivo central intercambió claves de seguridad apropiadas con el dispositivo periférico en respuesta a la solicitud de seguridad; en respuesta a un hallazgo negativo para la segunda determinación de autenticación, rechazar la solicitud de emparejamiento con el dispositivo periférico; y en respuesta a un hallazgo positivo para la segunda determinación de autenticación, completar el emparejamiento entre el dispositivo periférico y el dispositivo central para crear el canal de comunicación inalámbrica emparejada.

En un ejemplo, la solicitud de seguridad puede ser para al menos uno de un rasgo característico de seguridad de intermediario (MITM) y un rasgo característico de seguridad de vinculación.

60 En un ejemplo, el rasgo característico solicitado puede ser una clave de acceso predefinida.

En un ejemplo, las instrucciones para determinar la determinación de autenticación antes del emparejamiento de dispositivos en base a si el rasgo característico solicitado recibido por el dispositivo periférico es correcto para lograr una de una determinación satisfactoria y una determinación de coincidencia no satisfactoria pueden comprender instrucciones para determinar si la clave de acceso predefinida recibida por el dispositivo periférico coincide con un valor dispuesto previamente.

65

En un ejemplo, el rasgo característico solicitado puede ser una matriz de datos fuera de banda (OOB) predefinida.

5 En un ejemplo, las instrucciones para determinar la determinación de autenticación antes del emparejamiento de dispositivos en base a si el rasgo característico solicitado recibido por el dispositivo periférico es correcto para lograr una de una determinación satisfactoria y una determinación de coincidencia no satisfactoria pueden comprender instrucciones para determinar si la matriz de datos OOB predefinida recibida por el dispositivo periférico coincide con una matriz de datos OOB esperada.

10 En un ejemplo, el rasgo característico solicitado puede ser un valor predefinido de un modelo de asociación y las instrucciones para determinar la determinación de autenticación antes del emparejamiento de dispositivos en base a si el rasgo característico solicitado recibido por el dispositivo periférico es correcto para lograr una de una determinación satisfactoria y una determinación de coincidencia no satisfactoria pueden comprender instrucciones para determinar si el valor predefinido del modelo de asociación recibido por el dispositivo periférico coincide con un valor esperado del modelo de asociación.

15 En un ejemplo, el sistema de emparejamiento de dispositivos puede comprender además instrucciones para, en respuesta a un hallazgo negativo para la segunda determinación de autenticación, mostrar un mensaje indicativo del rechazo de la solicitud de emparejamiento en una pantalla de visualización del dispositivo periférico.

20 En un ejemplo que no forma parte de la invención como se reivindica, el sistema de emparejamiento de dispositivos puede incluir un dispositivo periférico, un dispositivo central, el sistema de emparejamiento de dispositivos configurado para emparejar el dispositivo periférico y el dispositivo central para establecer un canal de comunicación inalámbrica emparejada entre los mismos, uno o más procesadores, uno o más componentes de memoria acoplados de forma comunicativa al uno o más procesadores, e instrucciones legibles por máquina almacenadas en el uno o más componentes de memoria que provocan que el sistema de emparejamiento de dispositivos realice al menos lo siguiente cuando las ejecuta el uno o más procesadores: establecer una conexión a través de un canal de comunicación inalámbrica entre el dispositivo periférico y el dispositivo central; llevar a cabo, por el dispositivo central, un descubrimiento de características de GATT de un valor de característica del dispositivo periférico a través del canal de comunicación inalámbrica; enviar datos de autenticación desde el dispositivo central al dispositivo periférico indicativos de una primera determinación de autenticación; utilizar el dispositivo central para enviar una solicitud de emparejamiento al dispositivo periférico para iniciar el emparejamiento a través del canal de comunicación inalámbrica en base a la primera determinación de autenticación; determinar una segunda determinación de autenticación antes del emparejamiento de dispositivos en base a si los datos de autenticación indican que la segunda autenticación es satisfactoria o no satisfactoria; en respuesta a que la segunda determinación de autenticación sea no satisfactoria, rechazar la solicitud de emparejamiento con el dispositivo periférico; en respuesta a que la segunda determinación de autenticación sea satisfactoria, aprobar la solicitud de emparejamiento con el dispositivo periférico y enviar una respuesta de emparejamiento al dispositivo central; y emparejar el dispositivo central y el dispositivo periférico en base a la respuesta de emparejamiento para crear el canal de comunicación inalámbrica emparejada.

45 En un ejemplo, las instrucciones para enviar datos de autenticación desde el dispositivo central al dispositivo periférico indicativos de una primera determinación de autenticación pueden comprender instrucciones para escribir un valor por el dispositivo central en el valor de característica del dispositivo periférico, en el que un acontecimiento de escritura comprende la primera determinación de autenticación.

50 En un ejemplo, las instrucciones para determinar una segunda determinación de autenticación antes del emparejamiento de dispositivos en base a si los datos de autenticación indican que la segunda autenticación es satisfactoria o no satisfactoria pueden comprender instrucciones para determinar si el valor escrito en el valor de característica del dispositivo periférico coincide con un valor dispuesto previamente para lograr una de una determinación de coincidencia satisfactoria indicativa de que la segunda determinación de autenticación fue satisfactoria y una determinación de coincidencia no satisfactoria indicativa de que la segunda determinación de autenticación fue no satisfactoria.

55 En un ejemplo, las instrucciones para enviar datos de autenticación desde el dispositivo central al dispositivo periférico indicativos de una primera determinación de autenticación pueden comprender instrucciones para enviar datos de autenticación del dispositivo en respuesta a una solicitud de datos de autenticación del dispositivo desde el dispositivo periférico.

60 Cabe señalar que las menciones en el presente documento de un componente de la presente divulgación que se "configura" o "programa" de una forma particular, para realizar una propiedad particular, o funcionar de una manera particular, son menciones estructurales, a diferencia de las menciones del uso previsto. Más específicamente, las referencias en el presente documento a la manera en que se "configura" o "programa" un componente indican una condición física existente del componente y, como tal, se ha de tomar como una mención definitiva de las características estructurales del componente.

65

5 Cabe señalar que los términos "sustancialmente", "alrededor de" y "aproximadamente" se pueden utilizar en el presente documento para representar el grado inherente de incertidumbre que se puede atribuir a cualquier comparación, valor, medición u otra representación cuantitativa. Estos términos también se utilizan en el presente documento para representar el grado en que una representación cuantitativa puede variar con respecto a una referencia establecida sin dar como resultado un cambio en la función básica de la materia objeto en cuestión.

10 A menos que se defina de otro modo, todos los términos técnicos y científicos usados en el presente documento tienen el significado entendido habitualmente por un experto en la técnica a la que pertenece la presente divulgación. Como se usan en el presente documento, los artículos "un/uno" y "una" se refieren a uno o a más de uno (es decir, a al menos uno) del objeto gramatical del artículo. A modo de ejemplo, "un elemento" quiere decir un elemento o más de un elemento. Cabe señalar que el alcance de protección conferida a la presente invención descrita en el presente documento está delimitado por las reivindicaciones adjuntas.

REIVINDICACIONES

1. Un sistema de emparejamiento de dispositivos (100), que comprende:
- 5 - un dispositivo periférico (102) configurado para anunciar uno o más paquetes de datos;
- un dispositivo central (104) configurado para escanear y recibir el uno o más paquetes de datos, el sistema de emparejamiento de dispositivos (100) configurado para emparejar el dispositivo periférico (102) y el dispositivo central (104) para establecer un canal de comunicación inalámbrica emparejada entre los mismos;
- 10 - uno o más procesadores;
- uno o más componentes de memoria acoplados de forma comunicativa al uno o más procesadores; y
- 15 - instrucciones legibles por máquina almacenadas en el uno o más componentes de memoria que provocan que el sistema de emparejamiento de dispositivos realice al menos lo siguiente cuando las ejecuta el uno o más procesadores:
- establecer una conexión a través de un canal de comunicación inalámbrica que comprende un canal Bluetooth entre el dispositivo periférico (102) y el dispositivo central (104);
- 20 - llevar a cabo, por el dispositivo central (104), un descubrimiento de características de GATT de un valor de característica de GATT de un servicio de GATT del dispositivo periférico (102) a través del canal de comunicación inalámbrica;
- 25 - determinar una determinación de autenticación por el dispositivo periférico (102) antes del emparejamiento de dispositivos en base a la determinación de un valor de característica de GATT central del dispositivo central (104) por el dispositivo periférico (102) para lograr una de una determinación de coincidencia satisfactoria y una determinación de coincidencia no satisfactoria, en la que el valor de característica de GATT central es uno de un valor de característica de DIS o un identificador único universal (UUID);
- 30 - utilizar el dispositivo central (104) para enviar una solicitud de emparejamiento al dispositivo periférico (102) para iniciar el emparejamiento a través del canal de comunicación inalámbrica en base al descubrimiento de características de GATT del valor de característica de GATT del servicio de GATT del dispositivo periférico (102);
- 35 - en respuesta a la determinación de coincidencia no satisfactoria por el dispositivo periférico (102) como determinación de autenticación, rechazar la solicitud de emparejamiento con el dispositivo periférico (102);
- en respuesta a la determinación de coincidencia satisfactoria por el dispositivo periférico como determinación de autenticación, aprobar la solicitud de emparejamiento con el dispositivo periférico (102) y enviar una respuesta de emparejamiento al dispositivo central (104); y
- 40 - emparejar el dispositivo central (104) y el dispositivo periférico (102) en base a la respuesta de emparejamiento para crear el canal de comunicación inalámbrica emparejada.
- 45
2. El dispositivo de emparejamiento de dispositivos de la reivindicación 1, en el que el valor de característica de GATT del servicio de GATT del dispositivo periférico (102) comprende un valor de característica de un servicio de información del dispositivo (DIS) del dispositivo periférico (102).
- 50
3. El sistema de emparejamiento de dispositivos de la reivindicación 1 o 2, en el que las instrucciones para determinar una determinación de autenticación antes del emparejamiento de dispositivos en base a la determinación de un valor de característica de GATT central del dispositivo central (104) para lograr una de una determinación de coincidencia satisfactoria y una coincidencia no satisfactoria comprenden instrucciones para:
- 55 - llevar a cabo, por el dispositivo periférico (102), un descubrimiento de características de GATT de un valor de característica central del dispositivo central (104) a través del canal de comunicación inalámbrica;
- leer el valor de característica central por el dispositivo periférico (102) para establecer el valor de característica central como el valor de característica de GATT central;
- 60 - determinar la determinación de coincidencia satisfactoria en base al valor característico de GATT central que coincide con un valor dispuesto previamente según lo determinado por el dispositivo periférico (102); y
- determinar la determinación de coincidencia no satisfactoria en base al valor característico de GATT central que no coincide con un valor dispuesto previamente según lo determinado por el dispositivo periférico (102).
- 65

4. El sistema de emparejamiento de dispositivos de al menos una de las reivindicaciones precedentes, en el que las instrucciones para determinar una determinación de autenticación antes del emparejamiento de dispositivos en base a la determinación de un valor de característica de GATT central para lograr una de una determinación de coincidencia satisfactoria y una coincidencia no satisfactoria comprenden instrucciones para:
- 5
- utilizar el dispositivo central (104) para escribir el un valor de característica central en un valor de característica del dispositivo periférico (102) para establecer el valor de característica central como el valor de característica de GATT central;
- 10
- determinar la determinación de coincidencia satisfactoria en base al valor característico de GATT central que coincide con un valor dispuesto previamente según lo determinado por el dispositivo periférico (102); y
 - determinar la determinación de coincidencia no satisfactoria en base al valor característico de GATT central que no coincide con un valor dispuesto previamente según lo determinado por el dispositivo periférico (102).
- 15
5. El sistema de emparejamiento de dispositivos de la reivindicación 4, en el que el valor de característica de GATT central comprende un número de serie del dispositivo periférico (102) presentado desde el dispositivo periférico (102) al dispositivo central (104).
- 20
6. El sistema de emparejamiento de dispositivos de la reivindicación 5, que comprende además instrucciones para transmitir el número de serie del dispositivo periférico (102) desde el dispositivo periférico (102) al dispositivo central (104) a través del canal de comunicación inalámbrica.
- 25
7. El sistema de emparejamiento de dispositivos de al menos una de las reivindicaciones precedentes, en el que las instrucciones comprenden además instrucciones para intercambiar uno o más rasgos característicos de clave de seguridad entre el dispositivo central (104) y el dispositivo periférico (102) antes de emparejar el dispositivo central (104) y el dispositivo periférico (102).
- 30
8. El sistema de emparejamiento de dispositivos de la reivindicación 7, que comprende además instrucciones para vincular el dispositivo periférico (102) y el dispositivo central (104) de modo que, después de emparejar el dispositivo periférico (102) y el dispositivo central (104), almacenen el uno o más rasgos característicos de clave de seguridad que se intercambian.
- 35
9. El sistema de emparejamiento de dispositivos de la reivindicación 8, que comprende además instrucciones para desconectar el dispositivo periférico (102) y el dispositivo central (104) después de la vinculación.
- 40
10. El sistema de emparejamiento de dispositivos de al menos una de las reivindicaciones precedentes, en el que las instrucciones para establecer una conexión a través de un canal de comunicación inalámbrica entre el dispositivo periférico (102) y el dispositivo central (104) comprenden además instrucciones para colocar cada uno del dispositivo periférico (102) y el dispositivo central (104) en un modo de emparejamiento.
- 45
11. El sistema de emparejamiento de dispositivos de al menos una de las reivindicaciones precedentes, que comprende además instrucciones para:
- poner en marcha un temporizador de autenticación al comienzo del descubrimiento de características de GATT;
 - deshabilitar el temporizador de autenticación en respuesta a la determinación de coincidencia satisfactoria como determinación de autenticación; y
- 50
- mostrar una confirmación de emparejamiento en una pantalla de visualización respectiva de cada uno del dispositivo central (104) y el dispositivo periférico (102) después de emparejar el dispositivo central (104) y el dispositivo periférico (102) en base a la respuesta de emparejamiento.
- 55
12. Un sistema de emparejamiento de dispositivos (100) que comprende:
- un dispositivo periférico (102) configurado para anunciar uno o más paquetes de datos;
 - un dispositivo central (104) configurado para escanear y recibir el uno o más paquetes de datos, el sistema de emparejamiento de dispositivos (100) configurado para emparejar el dispositivo periférico (102) y el dispositivo central (104) para establecer un canal de comunicación inalámbrica emparejada entre los mismos;
 - uno o más procesadores;
- 60
- uno o más componentes de memoria acoplados de forma comunicativa al uno o más procesadores; y
- 65

- instrucciones legibles por máquina almacenadas en el uno o más componentes de memoria que provocan que el sistema de emparejamiento de dispositivos (100) realice al menos lo siguiente cuando las ejecuta el uno o más procesadores:
- 5
- establecer una conexión a través de un canal de comunicación inalámbrica que comprende un canal Bluetooth entre el dispositivo periférico (102) y el dispositivo central (104);
- 10
- llevar a cabo, por el dispositivo central (104), un descubrimiento de características de GATT de un valor de característica del dispositivo periférico (102) a través del canal de comunicación inalámbrica;
 - enviar un rasgo característico solicitado de al menos un valor de característica de GATT central del dispositivo central (104) desde el dispositivo central (104) al dispositivo periférico (102) para determinar una determinación de autenticación;
- 15
- determinar la determinación de autenticación por el dispositivo periférico (102) antes del emparejamiento de dispositivos en base a si el rasgo característico solicitado del al menos un valor de característica de GATT central del dispositivo central (104) según lo solicitado y recibido por el dispositivo periférico (102) es correcto para lograr una de una determinación satisfactoria y una determinación de coincidencia no satisfactoria, en la que el al menos un valor de característica de GATT central es uno de un valor de característica de DIS o un identificador único universal (UUID);
- 20
- utilizar el dispositivo central (104) para enviar una solicitud de emparejamiento al dispositivo periférico (102) para iniciar el emparejamiento a través del canal de comunicación inalámbrica en base al descubrimiento de características de GATT del dispositivo periférico (102) y la determinación de autenticación;
- 25
- en respuesta a un hallazgo incorrecto para la determinación de autenticación por el dispositivo periférico, rechazar la solicitud de emparejamiento con el dispositivo periférico (102);
- 30
- en respuesta a un hallazgo correcto para la determinación de autenticación por el dispositivo periférico, enviar una respuesta de emparejamiento inicial por el dispositivo periférico (102) que incluye una solicitud de seguridad y proceder a una segunda determinación de autenticación;
- 35
- determinar en la segunda determinación de autenticación si el dispositivo central (104) intercambié claves de seguridad apropiadas con el dispositivo periférico (102) en respuesta a la solicitud de seguridad;
 - en respuesta a un hallazgo negativo para la segunda determinación de autenticación, rechazar la solicitud de emparejamiento con el dispositivo periférico (102); y
- 40
- en respuesta a un hallazgo positivo para la segunda determinación de autenticación, completar el emparejamiento entre el dispositivo periférico (102) y el dispositivo central (104) para crear el canal de comunicación inalámbrica emparejada.
- 45
13. El sistema de emparejamiento de dispositivos de la reivindicación 12, en el que la solicitud de seguridad es para al menos un rasgo característico de seguridad de intermediario (MITM) y un rasgo característico de seguridad de vinculación.

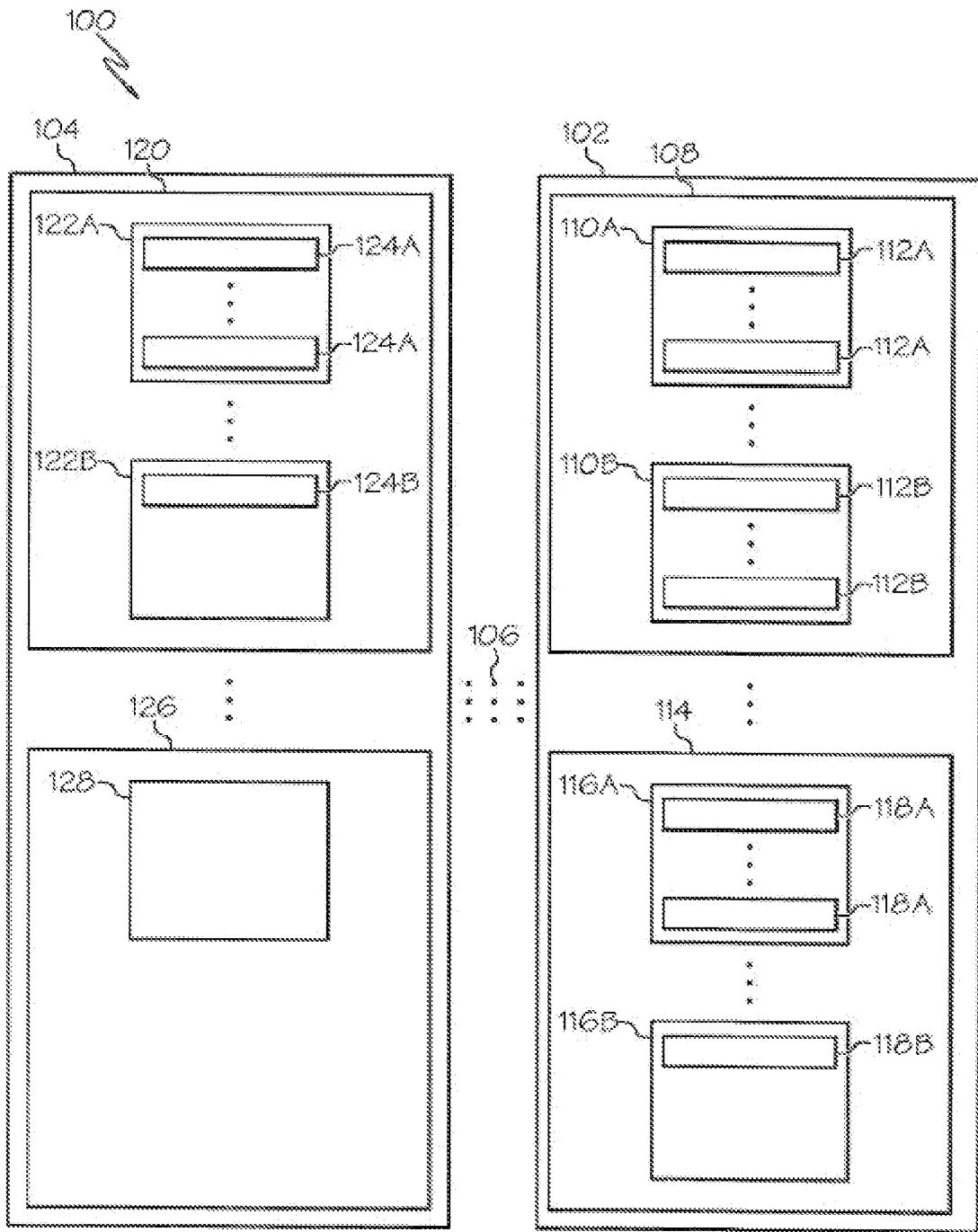


FIG. 1

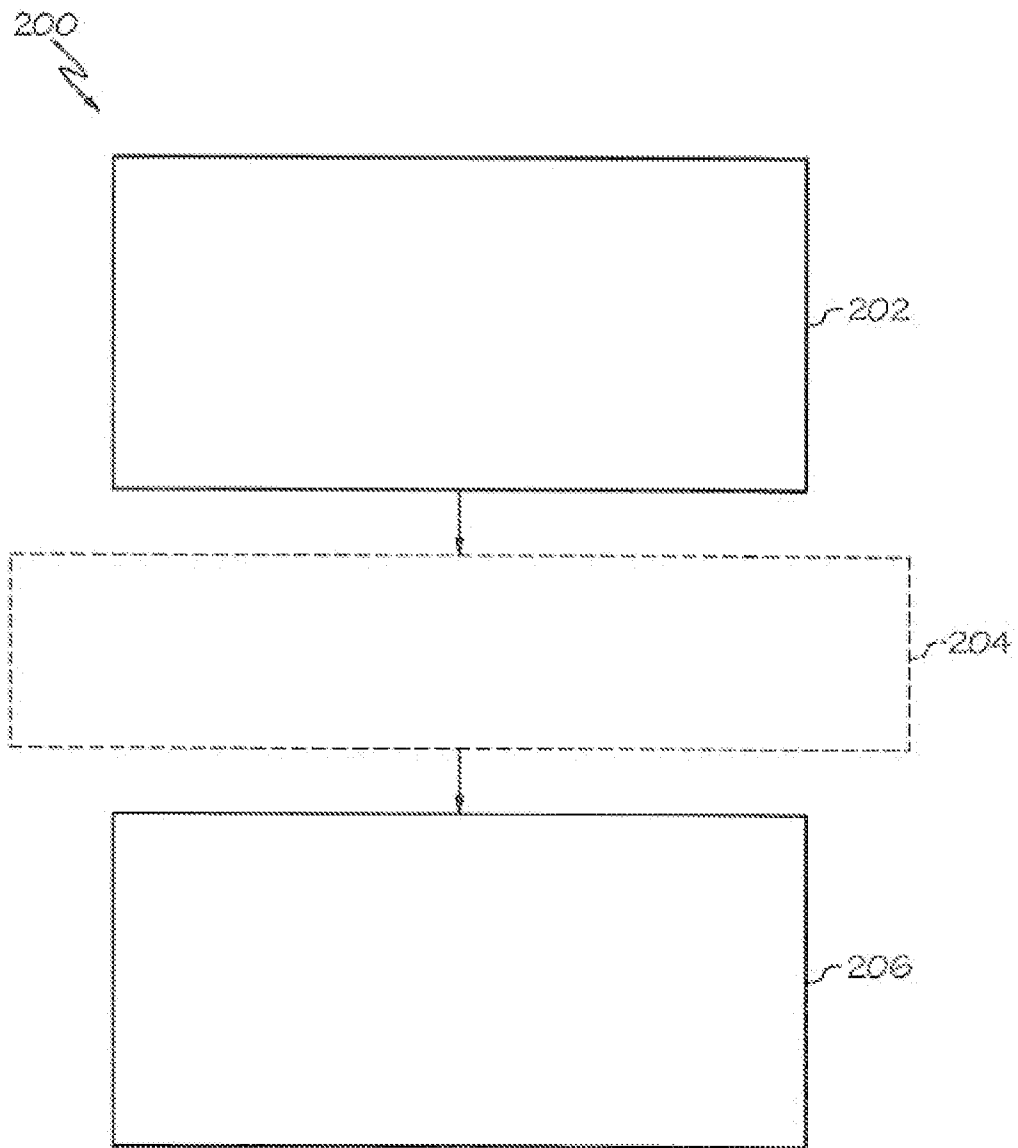


FIG. 2

302

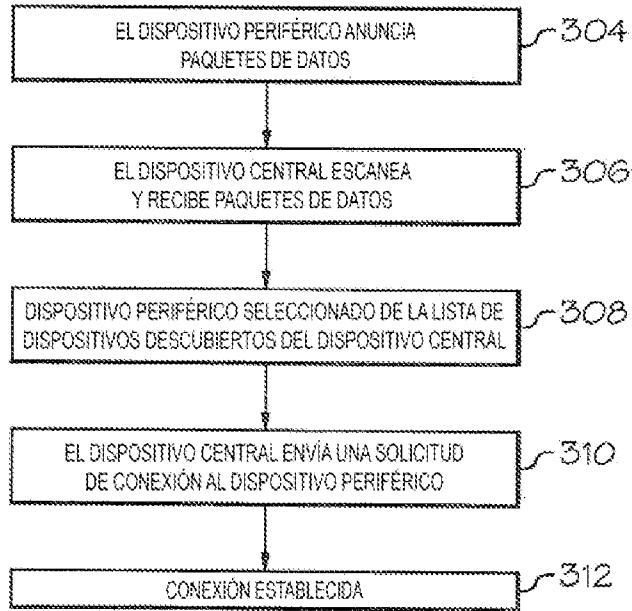


FIG. 3

406 ↘

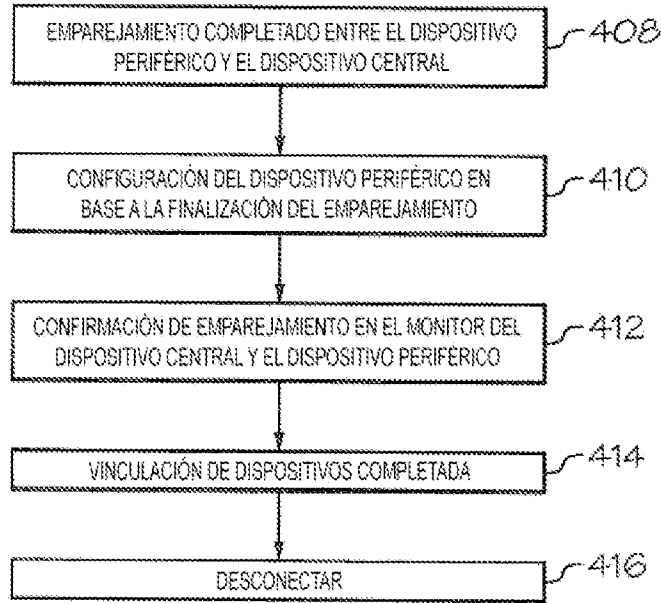


FIG. 4

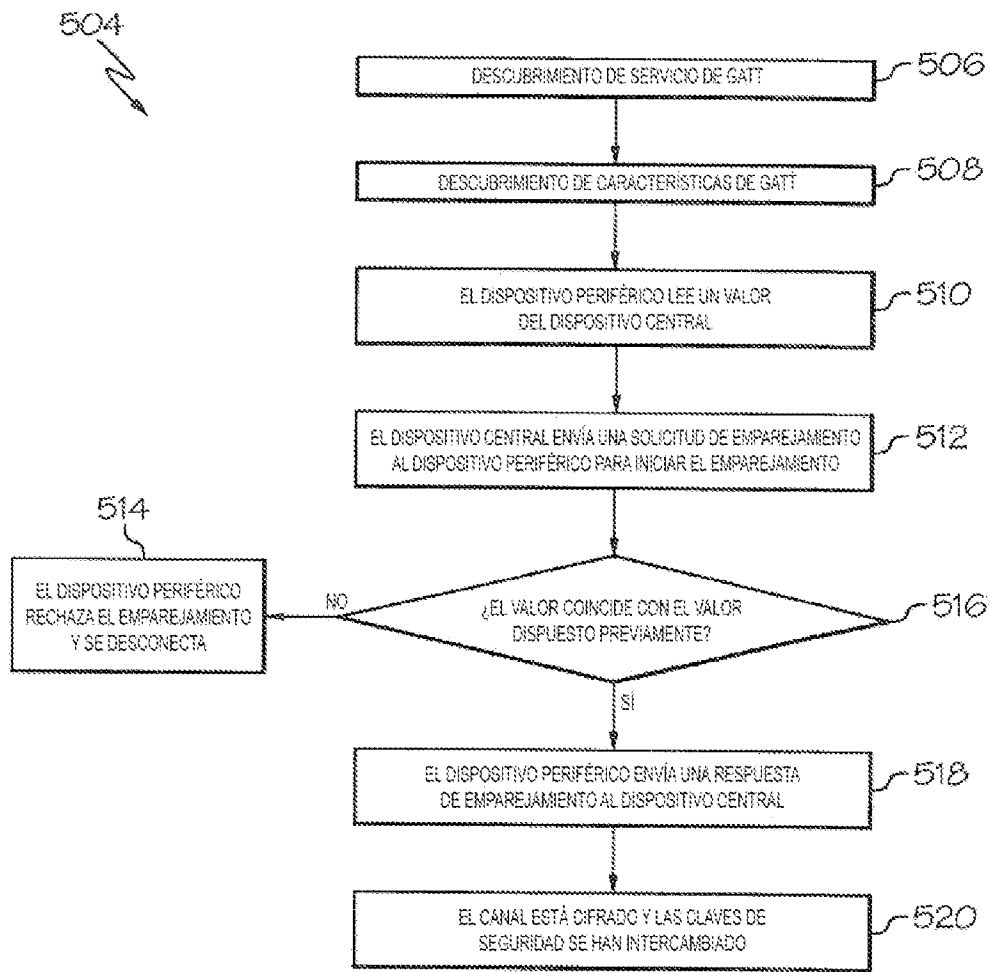


FIG. 5

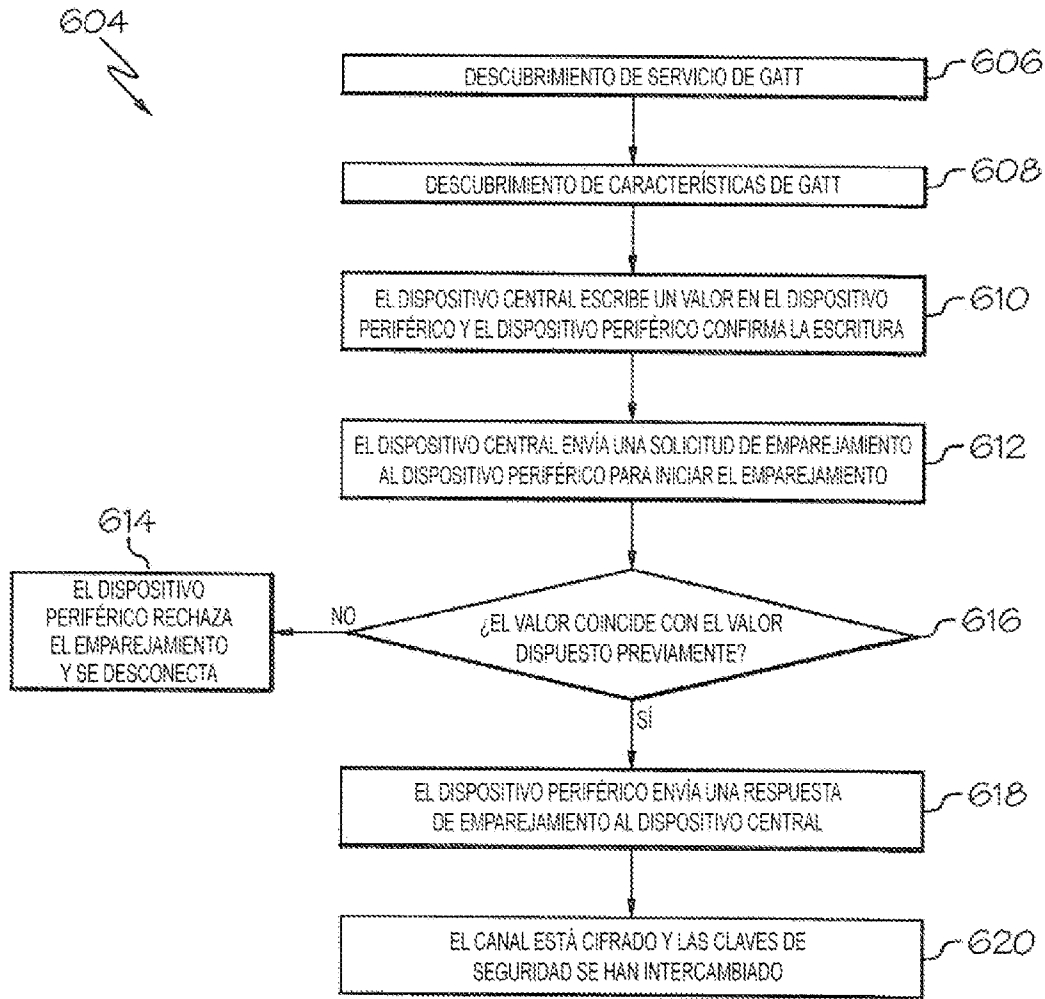


FIG. 6

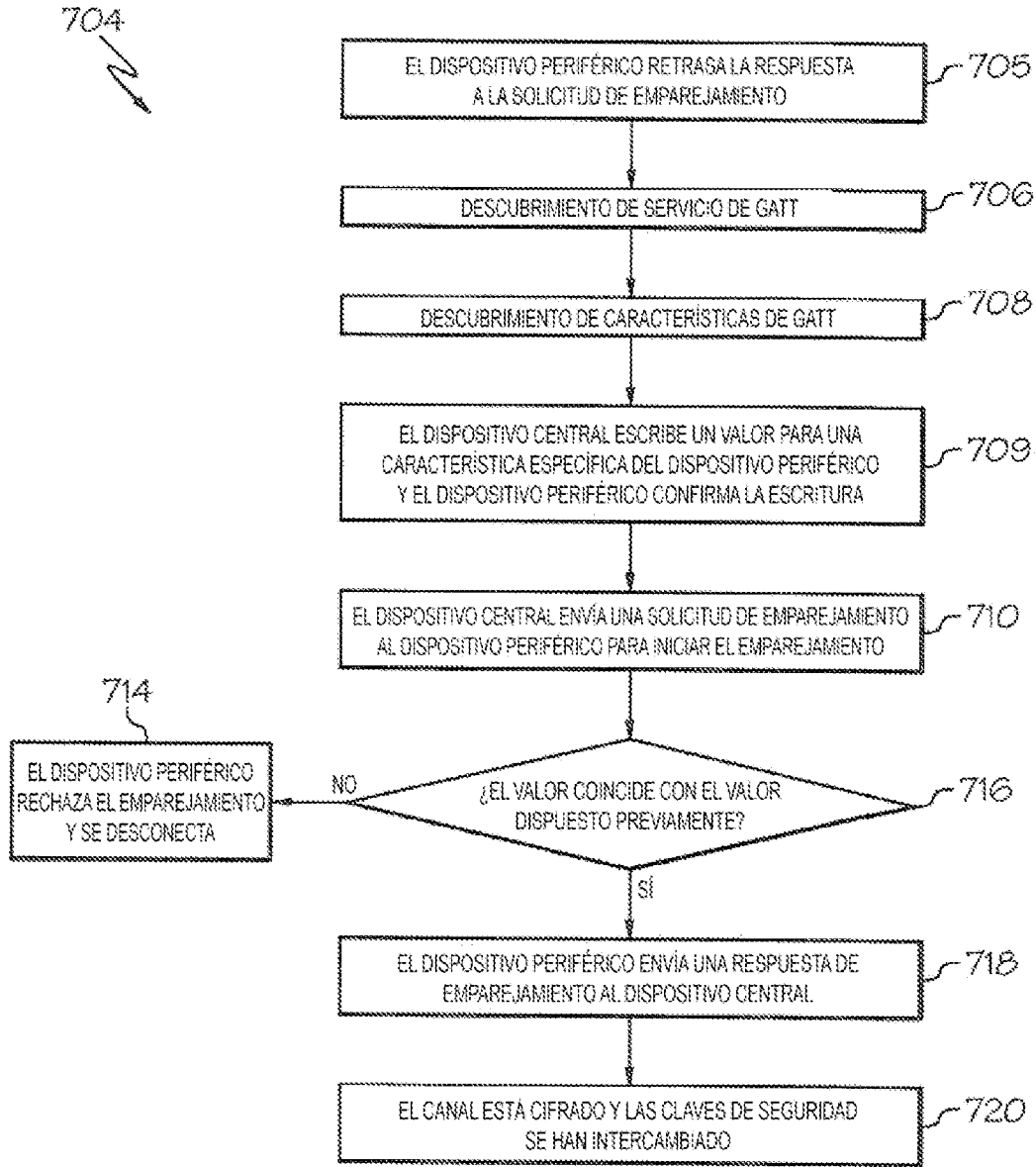


FIG. 7

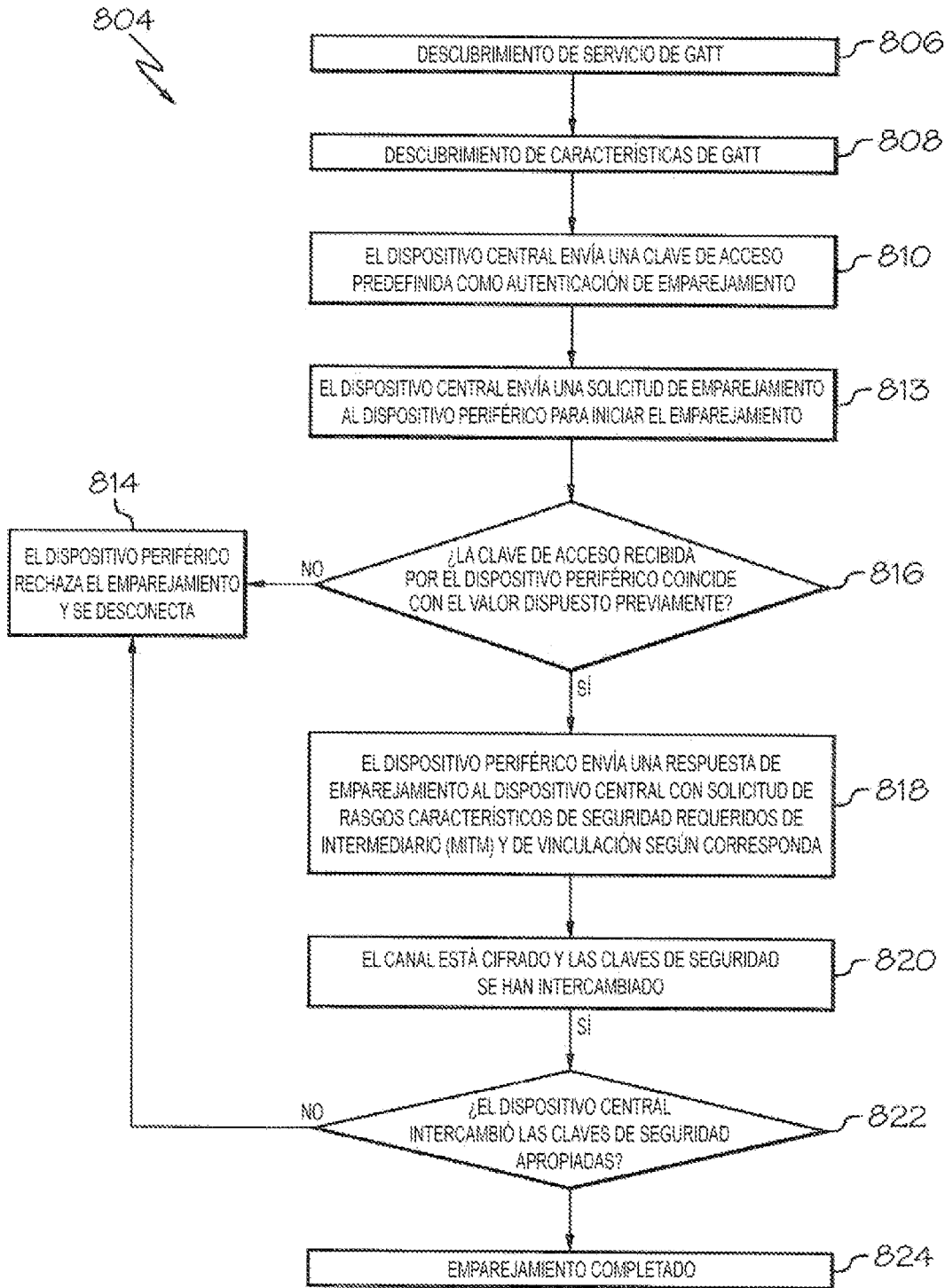


FIG. 8

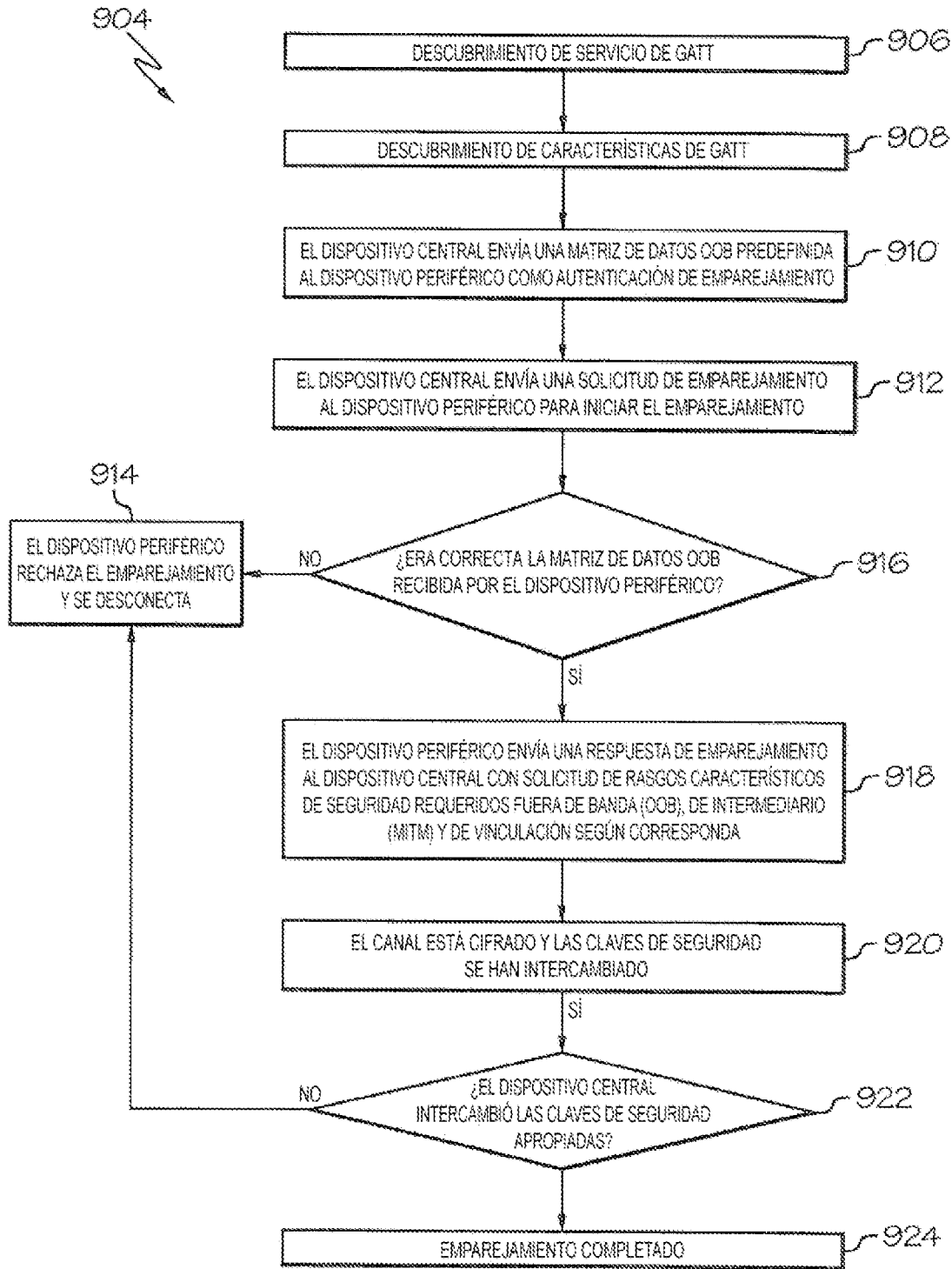


FIG. 9

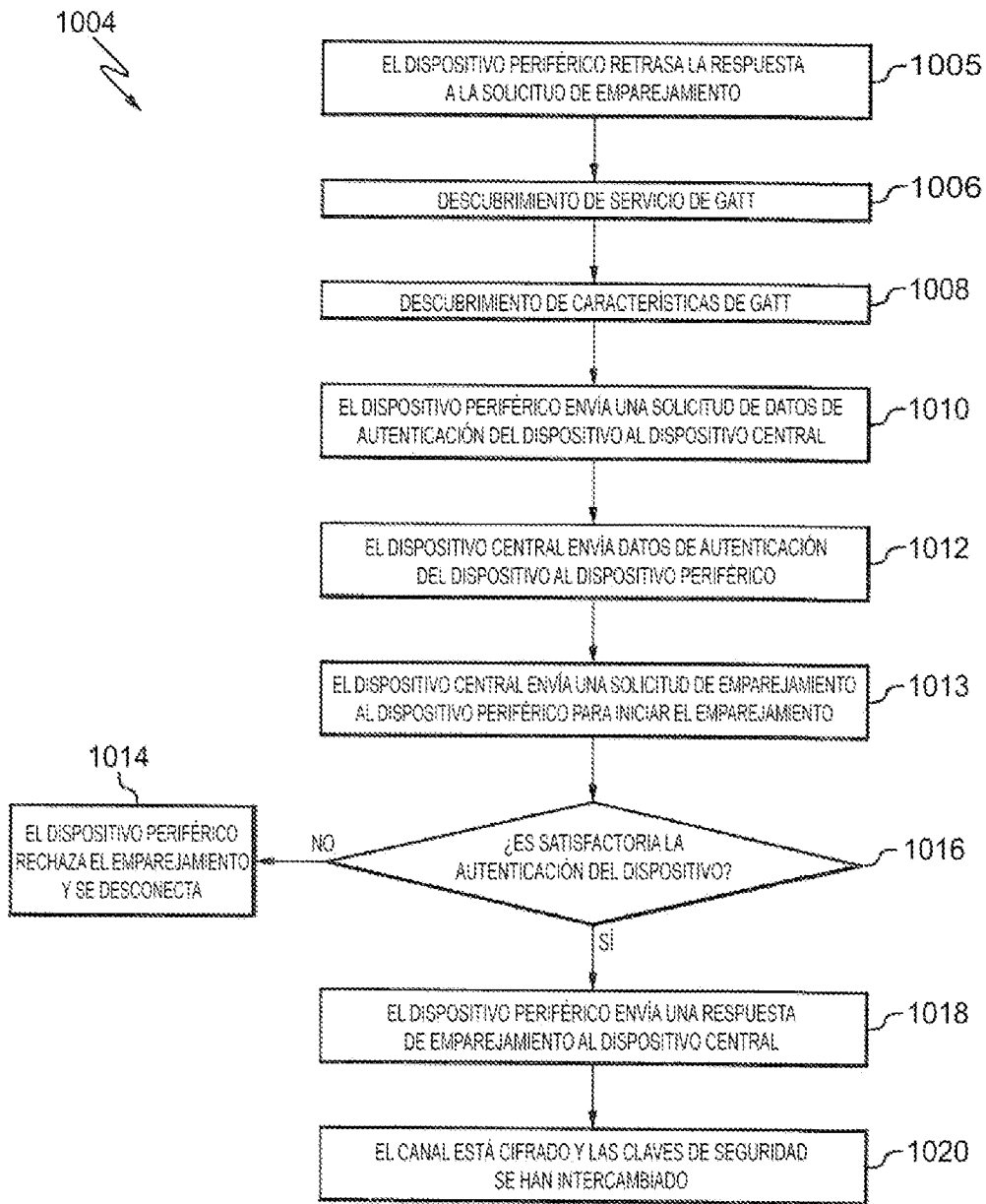


FIG. 10

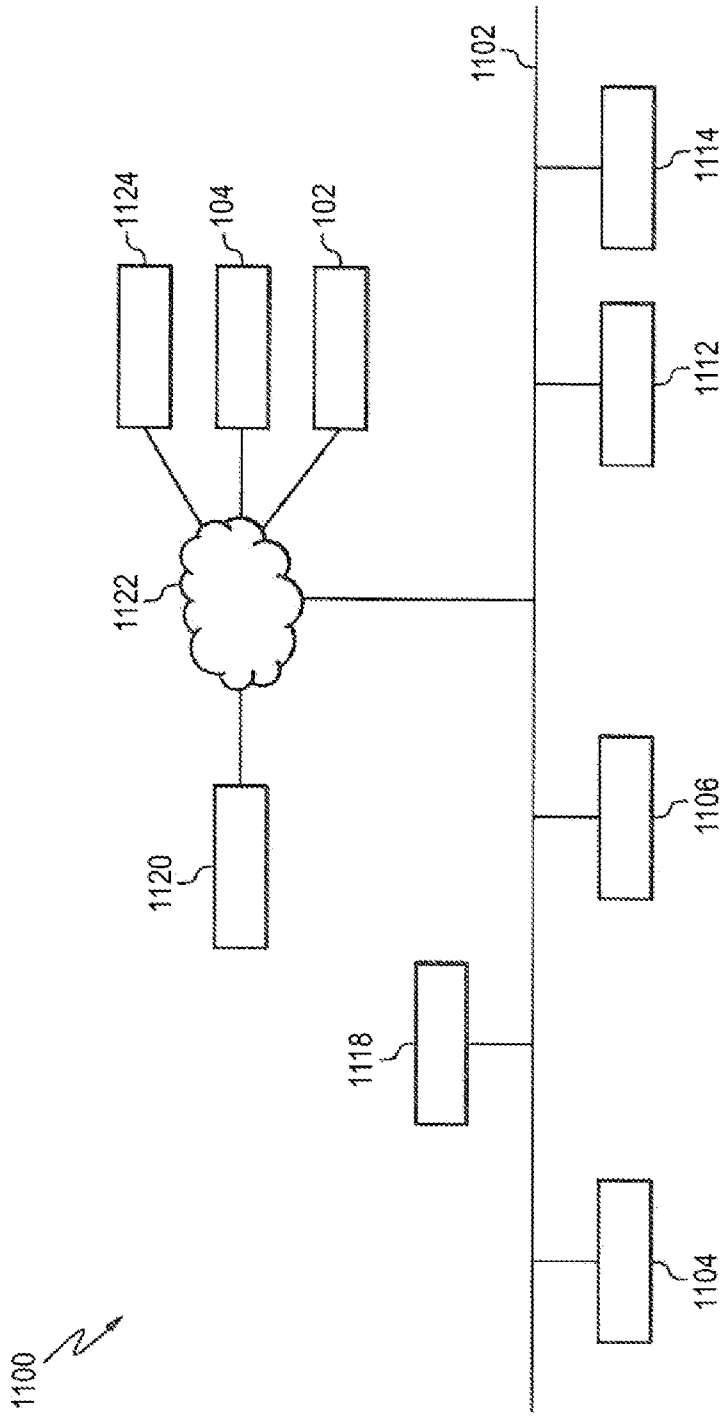


FIG. 11