(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 638 663**

(51) Int. CI.:

H04W 12/06 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **19.06.2014 E 14173104 (2)**

(97) Fecha y número de publicación de la concesión europea: **26.07.2017 EP 2958354**

(54) Título: **Emparejamiento de dispositivos**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
23.10.2017

(73) Titular/es:

NOKIA TECHNOLOGIES OY (100.0%)
Karaportti 3
02610 Espoo, FI

(72) Inventor/es:

REUNAMÄKI, JUKKA y
PALIN, ARTO

(74) Agente/Representante:

VALLEJO LÓPEZ, Juan Pedro

DESCRIPCIÓN

Emparejamiento de dispositivos

Campo técnico

El ejemplo y las realizaciones no limitantes de la presente invención se refieren al descubrimiento, selección y emparejamiento de dispositivos en el contexto de la comunicación inalámbrica.

Antecedentes

Establecer una conexión inalámbrica entre dos dispositivos, incluyendo, por ejemplo, las etapas del descubrimiento del dispositivo, la selección del dispositivo y la configuración de la conexión es en muchas ocasiones una operación complicada. Multitud de diferentes técnicas de comunicación, protocolos de comunicación y componentes de interfaz de usuario para controlar el uso de estas técnicas/protocolos pueden hacer que sea incómodo o incluso difícil para un usuario de un dispositivo llevar a cabo con éxito las etapas requeridas para establecer una conexión.

El emparejamiento de dispositivos es una técnica que se ha desarrollado para facilitar el establecimiento de conexiones entre dispositivos inalámbricos de manera segura cuando se utiliza una técnica de comunicación inalámbrica de corto alcance, como Bluetooth (BT) o WLAN (red de área local inalámbrica) según un estándar IEEE 802.11. En el emparejamiento de dispositivos, dos dispositivos, por ejemplo, un dispositivo de usuario y un punto de acceso o un dispositivo de usuario y un dispositivo accesorio, en el curso de un procedimiento de selección de dispositivo y un procedimiento de establecimiento de conexión entre los dispositivos crean una clave secreta compartida que también puede denominarse clave de autenticación o una clave de enlace.

El proceso de emparejamiento puede estar seguido por un proceso de unión, que implica almacenar la clave de enlace en los dos dispositivos que se utilizarán para la autenticación en procedimientos subsiguientes de establecimiento de conexión entre los mismos dos dispositivos. En una solicitud de conexión posterior de un dispositivo emparejado y enlazado, la clave de enlace se puede aplicar para autenticar el otro dispositivo y, por lo tanto, la conexión puede establecerse de una manera segura sin necesidad de acción del usuario. En consecuencia, el proceso de emparejamiento y enlace contribuye a un establecimiento de conexión fácil de usar entre dispositivos, especialmente entre pares de dispositivos usados frecuentemente.

Sin embargo, mientras que el emparejamiento y la unión proporciona un enfoque fácil de usar, por ejemplo, para conectar de forma inalámbrica un dispositivo de usuario a puntos de acceso y dispositivos accesorios que se usan regularmente, el proceso de emparejamiento y enlace que se basa en la clave de enlace puede no ser una solución conveniente para todos los escenarios de uso. A modo de ejemplo a este respecto, cuando un usuario tiene un primer dispositivo de usuario emparejado con uno o más dispositivos (por ejemplo, punto(s) de acceso y/o dispositivo(s) accesorio(s)) y desea establecer los mismos emparejamientos también para un segundo dispositivo de usuario, el proceso de vinculación y enlazado basado en clave de enlace debe llevarse a cabo por separado con el segundo dispositivo de usuario y cada uno de los otros dispositivos para crear las respectivas claves de enlace. Especialmente con un número elevado de otros dispositivos y/o en el caso de que los otros dispositivos requieran tomar acciones específicas del usuario para iniciar el emparejamiento, éste puede ser un proceso tedioso y que consume mucho tiempo.

Como otro ejemplo, si un primer dispositivo de usuario es compartido por un número de usuarios, pero el emparejamiento con ciertos otros dispositivos necesita estar limitado a uno o más usuarios seleccionados del primer dispositivo de usuario, el enfoque de clave de enlace puede no ser capaz de proporcionar la limitación deseada sin un mecanismo de autenticación de usuario adicional. Estos mecanismos, sin embargo, pueden complicar el diseño, la implementación y el uso del primer dispositivo de usuario y/o el uso de ciertos otros dispositivos, lo que puede ser inconveniente o incluso imposible, especialmente en el caso de dispositivos simples con capacidades (interfaz de usuario) limitadas.

En la técnica relacionada, WO 03/056746 A1 describe un método para establecer una conexión entre un primer dispositivo RF (radiofrecuencia) y un segundo dispositivo RF y una conexión entre el primer dispositivo RF y un tercer dispositivo RF, comprendiendo el método las etapas de inicializar la conexión entre el primer dispositivo RF y el segundo dispositivo, emparejando el primer dispositivo con el segundo dispositivo en un procedimiento de emparejamiento, dando como resultado que el primer dispositivo y el segundo dispositivo conozcan una clave de enlace (Ka). Además, establecer una conexión subsiguiente entre el primer dispositivo y el tercer dispositivo comprende las etapas de establecer una información de enlace que comprende la clave de enlace (Ka) y una identidad de enlace inicial, inicializar la conexión entre el primer dispositivo y el tercer dispositivo y asignar en el primer dispositivo, basado en la identidad de enlace inicial, siendo la clave de enlace (Ka), para el intercambio de mensajes entre el primer dispositivo y el tercer dispositivo.

"Bluetooth Security White Paper", Bluetooth SIG Security Expert Group, Revisión 1.00, del 19 de abril de 2002, páginas 1-46, describe el uso de la seguridad Bluetooth, así como el mecanismo de seguridad adicional para perfiles

inalámbricos Bluetooth seleccionados.

Sumario

Según una realización de la invención, se proporciona un aparato para la comunicación inalámbrica, comprendiendo el aparato medios para crear, en un procedimiento de emparejamiento con un primer dispositivo inalámbrico, una primera clave de autenticación dedicada a autenticar el primer dispositivo inalámbrico, medios para recibir, en el procedimiento con el primer dispositivo emparejado, una primera clave de autenticación por defecto para autenticar un dispositivo inalámbrico que no está emparejado con el aparato, medios para almacenar al menos dicha primera clave de autenticación por defecto para autenticar un dispositivo inalámbrico que no está emparejado con el aparato, medios para operar selectivamente el aparato en uno de estados predefinidos, comprendiendo dichos estados al menos un primer estado en el que el aparato es conectable pero no detectable por otros dispositivos inalámbricos, medios para recibir solicitudes de conexión de otros dispositivos inalámbricos, medios, en respuesta a la recepción, cuando el aparato es operado en dicho primer estado, una petición de conexión desde un segundo dispositivo inalámbrico que no está emparejado con el aparato, para verificar si dichas primeras claves de autenticación por defecto son una clave de autenticación válida para dicho segundo dispositivo inalámbrico, y medios, en respuesta a haber encontrado dicha primera clave de autenticación predeterminada como una clave de autenticación válida para dicha segunda conexión inalámbrica, para establecer una conexión autenticada con dicho segundo dispositivo inalámbrico.

De acuerdo con otra realización de la invención, se proporciona un método en un aparato para comunicación inalámbrica, comprendiendo el método crear, en un procedimiento de emparejamiento con un primer dispositivo inalámbrico, una primera clave de autenticación dedicada a autenticar el primer dispositivo inalámbrico, recibir, en el procedimiento con el primer dispositivo emparejado, una primera clave de autenticación predeterminada para autenticar un dispositivo inalámbrico que no está emparejado con el aparato, almacenar, al menos, dicha primera clave de autenticación predeterminada para autenticar un dispositivo inalámbrico que no está emparejado con el aparato; operar selectivamente el aparato en uno de los estados predefinidos, comprendiendo dichos estados al menos un primer estado en el que el aparato es conectable pero no detectable por otros dispositivos inalámbricos; verificar, en respuesta a haber recibido, cuando el aparato es operado en dicho primer estado, una solicitud de conexión desde un segundo dispositivo inalámbrico que no está emparejado con el aparato, si dicha primera clave de autenticación predeterminada es una clave de autenticación válida para dicho segundo dispositivo inalámbrico, y establecer, en respuesta a haber encontrado dicha primera clave de autenticación por defecto como una clave de autenticación válida para dicho segundo dispositivo inalámbrico, una conexión autenticada con dicho segundo dispositivo inalámbrico.

Según otra realización de la invención, se proporciona un programa informático, comprendiendo el programa de ordenador un código de programa legible por ordenador configurado para provocar la realización del método descrito en lo anterior cuando dicho código de programa es ejecutado en un aparato informático.

El programa de ordenador al que se ha hecho referencia anteriormente puede estar realizado en un medio de registro volátil o no volátil, por ejemplo como un producto de programa informático que comprende al menos un medio no transitorio legible por ordenador que tiene un código de programa almacenado en él, el programa que cuando es ejecutado por un aparato hace que el aparato al menos realice las operaciones descritas anteriormente en el presente documento para el programa informático de acuerdo con un ejemplo de realización de la invención.

Las realizaciones a modo de ejemplo de la invención presentadas en esta solicitud de patente no deben interpretarse como limitaciones de la aplicabilidad de las reivindicaciones adjuntas. El verbo "comprender" y sus derivados se utilizan en esta solicitud de patente como una limitación abierta que no excluye la existencia de rasgos no apreciados. Las características descritas a continuación se pueden combinar mutuamente libremente a menos que se indique explícitamente lo contrario.

Algunas características de la invención se exponen en las reivindicaciones adjuntas. Sin embargo, los aspectos de la invención, tanto en lo que respecta a su construcción como a su método de funcionamiento, junto con objetos y ventajas adicionales de la misma, se comprenderán mejor a partir de la siguiente descripción de algunas realizaciones de ejemplo cuando se lee en relación con los dibujos adjuntos.

Breve descripción de las figuras

Las realizaciones de la invención se ilustran a modo de ejemplo, y no a modo de limitación, en las figuras de los dibujos adjuntos.

La figura 1 ilustra esquemáticamente algunos componentes de un ejemplo de una disposición de comunicación inalámbrica.

La figura 2a ilustra esquemáticamente algunos componentes de un dispositivo de acuerdo con un ejemplo de realización.

La figura 2b ilustra esquemáticamente algunos componentes de un dispositivo de acuerdo con un ejemplo de realización.

La figura 3 ilustra un método de acuerdo con un ejemplo de realización.

La figura 4 ilustra un método de acuerdo con un ejemplo de realización.

La figura 5 ilustra un método de acuerdo con un ejemplo de realización.

Descripción de algunas formas de realización

Como se describe en la sección de antecedentes, el término emparejamiento se aplica aquí para referirse a dos dispositivos pares que crean u obtienen un secreto compartido al establecerse la conexión, mientras que el término unión se aplica en la presente memoria para referirse a los dispositivos pareados emparejados que almacenan el secreto compartido creado/obtenido con propósitos de autenticación en tentativas de conexión subsiguientes por el otro dispositivo emparejado y enlazado. A continuación, dicho secreto compartido creado/obtenido por los dos dispositivos iguales se denomina clave de autenticación o clave de enlace.

Por consiguiente, en un intento de conexión posterior por el dispositivo enlazado, el otro dispositivo ya está autentificado previamente y, por lo tanto, no es necesario llevar a cabo el procedimiento de emparejamiento de nuevo para autenticar al otro dispositivo, facilitando así el establecimiento de conexiones rápidas y seguras en un sistema automatizado o semiautomatizado. Por otra parte, si no se ha realizado la unión, puede realizarse un procedimiento de emparejamiento cada vez que se establece una conexión entre los dispositivos. Sin embargo, también el procedimiento de emparejamiento puede llevarse a cabo de una manera automatizada o semiautomática.

Además de almacenar la clave de enlace, el proceso de unión puede comprender además el almacenamiento de otra información sobre el dispositivo enlazado, por ejemplo, Una identificación del otro dispositivo (por ejemplo, una dirección MAC del dispositivo u otra dirección o identificador adecuado), una identificación de un usuario asociado al otro dispositivo (por ejemplo, un nombre de usuario, una dirección de correo electrónico u otro identificador adecuado)

La figura 1 ilustra esquemáticamente algunos componentes o entidades de una disposición de comunicación inalámbrica 100 para representar un marco a modo de ejemplo para una o más realizaciones de la presente invención. La disposición de comunicación 100 puede considerarse que representa un caso de uso en el que un primer dispositivo 110 y un segundo dispositivo 130 establecen o han establecido un emparejamiento y posiblemente uniones entre sí y, por tanto, crean o han creado una clave de enlace, llevan a cabo un procedimiento para definir la información de emparejamiento predeterminada que puede aplicarse para facilitar el establecimiento subsiguiente de la conexión al segundo dispositivo 130 por el primer dispositivo 110 y/u otro dispositivo y proporcionar la información de emparejamiento predeterminada a un dispositivo servidor 170 a través de una red 190. La información de emparejamiento puede comprender, por ejemplo, una clave de enlace predeterminada creada en el procedimiento entre los dispositivos 110 y 130 y/o información que identifica el primer dispositivo 110 y/o un usuario del mismo. Posteriormente, un tercer dispositivo 150 puede obtener la información de emparejamiento predeterminada desde el dispositivo servidor 170 y utilizar la información de emparejamiento predeterminada para establecer una conexión con el segundo dispositivo 130 y autenticarse sin necesidad de llevar a cabo el proceso de emparejamiento. En otras palabras, en este marco de ejemplo, el tercer dispositivo 150 está capacitado para reutilizar la información de emparejamiento predeterminada creada en el procedimiento entre el primer dispositivo 110 y el segundo dispositivo 130.

En la disposición de comunicación 100, se supone que la conexión entre el primer dispositivo 110 y el segundo dispositivo 130 y la conexión entre el tercer dispositivo 150 y el segundo dispositivo 130 es inalámbrica. La conexión entre el primer dispositivo 110 y la red 190 y la conexión entre el tercer dispositivo 150 y la red 190 puede ser una conexión por cable o inalámbrica. La conexión entre el dispositivo servidor 170 y la red 190 es normalmente, pero no necesariamente, una conexión cableada. La red 190 puede comprender, por ejemplo, una red de área personal (PAN), una red de área local (LAN) y/o una red de área amplia (WAN) tal como Internet.

Los componentes de la disposición de comunicación 100 proporcionan un ejemplo no limitativo que representa un único segundo dispositivo 130 y un único tercer dispositivo 150 para mayor claridad de la ilustración. Sin embargo, puede haber uno o más segundos dispositivos 130 y uno o más terceros dispositivos 150. A continuación, el término segundo dispositivo 130, cuando se usa en forma singular, se aplica para referirse conjuntamente a cualquiera de uno o más segundos dispositivos 130 a menos que se indique explícitamente lo contrario. De forma similar, el término tercer dispositivo 150, cuando se usa en forma singular, se aplica para referirse conjuntamente a cualquiera de uno o más terceros dispositivos 150 a menos que se indique explícitamente lo contrario.

Como escenario de ejemplo dentro del marco de la disposición de comunicación 100, un usuario determinado puede utilizar el primer dispositivo 110 para establecer el emparejamiento con el segundo dispositivo 130 y puede desear

crear y compartir la información de emparejamiento predeterminada asociada para ser reutilizada por uno o más Más terceros dispositivos 150 usados por el usuario determinado, evitando así la necesidad de llevar a cabo por separado el procedimiento de emparejamiento entre cada uno de los terceros dispositivos 150 usados por el usuario determinado y el segundo dispositivo 130. Tal escenario puede encontrarse, por ejemplo, cuando cada uno de los dispositivos primero y tercero 110, 150 es un dispositivo de usuario (por ejemplo, un teléfono móvil, un ordenador de tableta, un ordenador portátil, etc.) y utilizado por un cierto usuario y el segundo dispositivo 130 es un dispositivo accesorio (por ejemplo, una impresora, una pantalla, un dispositivo de entrada/salida de audio, un dispositivo sensor, etc.) que desea emparejar con cada uno de sus dispositivos de usuario.

Como otro escenario de ejemplo, un usuario puede establecer emparejamiento entre el primer dispositivo 110 y un número alto de segundos dispositivos 130 y puede desear crear y compartir la información de emparejamiento predeterminada asociada a uno o más terceros dispositivos 150. Tal escenario puede encontrarse, por ejemplo, cuando el primer dispositivo 110 es un dispositivo de usuario utilizado por un determinado usuario como su dispositivo primario emparejado con una serie de dispositivos accesorios y este usuario determinado adopta el tercer dispositivo 150 como su nuevo dispositivo de usuario principal y/o cuando el usuario determinado está introduciendo el tercer dispositivo 150 como un dispositivo de usuario adicional para su uso en paralelo con el primer dispositivo 110.

El primer dispositivo 110 es normalmente, pero no necesariamente, un dispositivo de usuario móvil. La figura 2a ilustra esquemáticamente algunos componentes de un primer dispositivo 110 que ejemplifica. El primer dispositivo 110 comprende una porción de comunicación inalámbrica 112 para comunicación inalámbrica con otros dispositivos. La porción de comunicación inalámbrica 112 puede permitir, por ejemplo, la comunicación con otros dispositivos utilizando una técnica o protocolo de comunicación inalámbrica de corto alcance que permita una conexión inalámbrica punto a punto con otro dispositivo. El primer dispositivo 110 es por tanto capaz de comunicarse con otros dispositivos que están equipados con medios de comunicación que utilizan la misma técnica/protocolo. La porción de comunicación inalámbrica 112 puede considerarse que incluye uno o más aparatos de comunicación inalámbrica incluidos en (o alojados por) el primer dispositivo 110 (o el primer aparato 110). La porción de comunicación inalámbrica 112 puede considerarse también como medios de comunicación inalámbrica 112.

El primer dispositivo 110 comprende además un procesador 116 y una memoria 115 para almacenar datos y un programa de ordenador 117. El primer dispositivo 110 puede comprender además componentes 118 de entrada/salida de usuario que pueden estar dispuestos, posiblemente junto con el procesador 116 y una porción del programa de ordenador 117, para proporcionar una interfaz de usuario para recibir la entrada de un usuario del primer dispositivo 110 y/o proporcionar salida al usuario del primer dispositivo 110. El procesador 116 puede estar dispuesto para controlar el funcionamiento del primer dispositivo 110, por ejemplo, de acuerdo con el programa de ordenador 117 almacenado en la memoria 115, de acuerdo con la entrada de usuario recibida a través de los componentes de E/S de usuario 118 y/o de acuerdo con la información recibida a través de la porción de comunicación inalámbrica 112. La memoria 115 y el programa de ordenador 117 almacenados en el mismo pueden estar además dispuestos para, con el procesador 116, proporcionar una función de control para controlar el funcionamiento de la porción de comunicación inalámbrica 112, posiblemente junto con una parte de control o una función de control que se puede proporcionar dentro de la porción de comunicación inalámbrica 112 (que se describirá más adelante en este texto). El primer dispositivo 110 puede comprender otros componentes o porciones además de los representados en la figura 2a.

El segundo dispositivo 130 puede ser un dispositivo móvil o un dispositivo fijo. La figura 2b ilustra esquemáticamente algunos componentes de un segundo dispositivo de ejemplo 130. El segundo dispositivo 130 comprende una porción de comunicación inalámbrica 132 similar a la porción de comunicación inalámbrica 112, la cual puede permitir, por ejemplo, la comunicación inalámbrica de corto alcance con el primer dispositivo 110 y/o con otros dispositivos equipados con medios de comunicación que utilizan la misma técnica /protocolo. A lo largo de las líneas descritas para la porción de comunicación inalámbrica 112, la porción de comunicación inalámbrica 132 puede considerarse que incluye uno o más aparatos de comunicación inalámbrica y la porción de comunicación inalámbrica 132 puede considerarse también como un medio de comunicación inalámbrica 132 incluido en (o alojado por) del segundo dispositivo 130.

El segundo dispositivo 130 comprende además un procesador 136 y una memoria 135 para almacenar datos y un programa de ordenador 137. El segundo dispositivo 130 puede comprender además componentes 138 de E/S (entrada/salida) de usuario 138 que pueden estar dispuestos, junto con el procesador 136 y una parte del programa de ordenador 137, para proporcionar una interfaz de usuario para recibir entrada de un usuario del segundo dispositivo 130 y/o proporcionar salida al usuario del segundo dispositivo 130. El procesador 136 puede estar dispuesto para controlar el funcionamiento del segundo dispositivo 130 de acuerdo con el programa de ordenador 137 almacenado en la memoria 135 y posiblemente más de acuerdo con la entrada de usuario recibida a través de los componentes de E/S de usuario y/o de acuerdo con la información recibida a través de la porción de comunicación inalámbrica 132. La memoria 135 y el programa de ordenador 137 almacenados en el mismo pueden estar además dispuestos para, con el procesador 136, controlar el funcionamiento de la porción de comunicación inalámbrica 132, posiblemente junto con una parte de control de una función de control que puede estar prevista dentro de la porción de comunicación respectiva 132 (que se describirá más adelante en este texto). El segundo

dispositivo 130 puede comprender otros componentes o porciones además de los representados en la figura 2b.

El tercer dispositivo 150 puede considerarse como un dispositivo que tiene una estructura similar al primer dispositivo 110 representado en la figura 2a. Para facilitar la posterior descripción de la operación ejemplificativa del tercer dispositivo 150 con referencias específicas a algunos de sus componentes, un componente del tercer dispositivo 150 correspondiente a un componente 11x del primer dispositivo 110 puede denominarse como los componentes 15x.

Cada una de las porciones de comunicación inalámbrica 112, 132, 152 puede comprender uno o más aparatos de comunicación respectivos. Se puede proporcionar un aparato de comunicación, por ejemplo, Como un chipset respectivo y/o como un módulo de comunicación respectivo. Para claridad y brevedad de la descripción, cada aparato de comunicación comprendido en la porción de comunicación inalámbrica 112, 132, 152 puede considerarse como una sola porción lógica que también puede ser capaz de procesar al menos parte de la información recibida a través de la conexión inalámbrica y/o al menos parte de la información que ha de transmitirse a través de la conexión inalámbrica sin control externo de otros componentes del dispositivo respectivo 110, 130, 150 (por ejemplo, del procesador 116, 136, 156). En una realización, cada uno de los aparatos de comunicación en la porción de comunicación inalámbrica 112, 132, 152 puede comprender, por ejemplo, una porción de transceptor inalámbrico para comunicación inalámbrica y una parte de control (o una función de control) para controlar el funcionamiento de la parte de transceptor inalámbrico respectiva y para procesar la información recibida/transmitida a través de la parte respectiva de transceptor inalámbrico. Dicha función de control puede proporcionarse mediante medios de hardware, por medio de software o por una combinación de medios de hardware y medios de software. Como ejemplo a este respecto, el aparato de comunicación inalámbrica puede comprender una memoria y un procesador, y un código de programa informático almacenado en la memoria puede estar dispuesto para proporcionar, con el procesador, la función de control para controlar el funcionamiento del respectivo aparato de comunicación inalámbrica Independientemente o conjuntamente con la función de control proporcionada por la memoria 115, 135, 155, el programa informático 117, 137, 157 y el procesador 116, 136, 157 del dispositivo 110, 130, 150 respectivo.

La conexión inalámbrica entre las porciones de comunicación inalámbrica 112 y 132 y/o entre las porciones de comunicación inalámbrica 152 y 132 puede proporcionarse empleando un procedimiento o protocolo de comunicación inalámbrica de corto alcance adecuado. El término comunicación inalámbrica de corto alcance, tal como se utiliza en la presente memoria, se refiere a una técnica o protocolo de comunicación inalámbrica que permite un rango operativo típico en la escala de decenas de metros, por ejemplo, hasta 100 metros. Sin embargo, especialmente en un entorno interior, el alcance operativo de tal técnica/protocolo de comunicación inalámbrica de corto alcance puede ser significativamente más corto, por ejemplo, debido a paredes y otras estructuras fijas, así como a muebles, etc., que son susceptibles de bloquear parcialmente o interferir con la comunicación por radio entre las porciones de comunicación inalámbrica 112 y 132. Por otra parte, en condiciones favorables en el uso al aire libre el alcance operacional puede extenderse a varios centenares de metros. Ejemplos de tales técnicas/protocolos inalámbricos incluyen los protocolos Bluetooth (BT) Básico/Mejorado de Datos (BR/EDR) y los protocolos Bluetooth Low Energy (BLE) especificados, por ejemplo, en la versión 4.1 de la especificación Bluetooth, paquete básico cubierto 4.1 (fecha de publicación 3 de diciembre de 2013). A continuación, este documento se conoce como una especificación Bluetooth. Otros ejemplos de técnicas/protocolos inalámbricos de corto alcance aplicables incluyen, por ejemplo, protocolos ZigBee (IEEE 802.15.4) y Z-Wave.

Aunque una serie de técnicas/protocolos de comunicación inalámbrica de corto alcance conocidos en la técnica son aplicables en el marco de la disposición de comunicación 100, a continuación, se describen algunos aspectos de varias realizaciones de la presente invención con referencias al protocolo BT BR/EDR. Sin embargo, el BT BR/EDR sirve como un ejemplo ilustrativo y no limitativo a este respecto, y la descripción se generaliza en cualquier protocolo de comunicación inalámbrica en el que el primer dispositivo 110 y el segundo dispositivo 130 son capaces de establecer un emparejamiento entre sí en el significado descrito en lo anterior.

La figura 3 ilustra un método de ejemplo 300 para crear y compartir información de emparejamiento obtenida en un procedimiento de emparejamiento entre el primer dispositivo 110 y el segundo dispositivo 130 para permitir que el tercer dispositivo 150 descubra posteriormente el segundo dispositivo 130 y se autentique con el segundo dispositivo 130 de forma automatizada sin necesidad de implicación del usuario.

El funcionamiento del método 300 puede estar precedido por un descubrimiento inicial de dispositivo y selección de dispositivo, mientras que el método 300 puede llevarse a cabo durante y/o después de un establecimiento de conexión entre el primer dispositivo 110 y el segundo dispositivo 130.

A este respecto, para proporcionar el descubrimiento inicial del dispositivo, el segundo dispositivo 130 puede estar dispuesto para funcionar en un modo o estado en el que es detectable por otros dispositivos (por ejemplo, la operación de exploración de consulta del protocolo BT BR/EDR) y el primer dispositivo 110 puede estar dispuesto para transmitir uno o más mensajes, denominados mensajes de consulta, para descubrir otros dispositivos de tipo deseado y/o características deseadas y para explorar mensajes de respuesta enviados desde uno o más otros dispositivos en respuesta a los mensajes de consulta (por ejemplo, la operación de consulta del protocolo BT BR/EDR). El segundo dispositivo 130 puede estar dispuesto para transmitir, en respuesta a la recepción de uno o

más mensajes de consulta desde el primer dispositivo 110, una respuesta de consulta (por ejemplo, paquete de sincronización de salto de frecuencia (FHS) posiblemente seguido por un paquete de respuesta de consulta extendida (EIR) BT BR/EDR) que transporta la información requerida para el establecimiento de la conexión con el segundo dispositivo 130.

La selección inicial del dispositivo y el establecimiento de la conexión con un dispositivo no enlazado puede implicar que el usuario del primer dispositivo 110 realice, a través de la interfaz de usuario, una selección para establecer una conexión a un dispositivo, por ejemplo, el segundo dispositivo 130, encontrado en la fase inicial de detección de dispositivos. A este respecto, el primer dispositivo 110 puede configurarse para mostrar, a través de la interfaz de usuario, al menos parte de la información recibida en la respuesta de consulta que se origina desde el segundo dispositivo 130 para permitir la selección del dispositivo encontrado, por ejemplo, el segundo dispositivo 130. Además, el primer dispositivo 110 puede estar dispuesto para recibir, a través de la interfaz de usuario, una selección de usuario para establecer una conexión con el segundo dispositivo 130 y, en consecuencia, establecer la conexión con el segundo dispositivo 130 en respuesta a la selección del usuario. El establecimiento de conexión puede implicar un procedimiento (por ejemplo, un procedimiento de búsqueda) para intercambiar información (adicional) requerida para el establecimiento de conexión entre el primer dispositivo 110 y el segundo dispositivo 130.

El método 300 procede de la fase de establecimiento de conexión entre el primer dispositivo 110 y el segundo dispositivo 130. El método 300 comienza con el apareamiento inicial entre el primer dispositivo 110 y el segundo dispositivo 130, como se indica en el bloque 310. El proceso de emparejamiento para establecer el emparejamiento inicial puede realizarse como parte del procedimiento de establecimiento de conexión o puede seguir el procedimiento de establecimiento de conexión.

En el transcurso del proceso de emparejamiento inicial, el primer dispositivo 110 y el segundo dispositivo 130 están dispuestos para crear un secreto compartido, es decir, una clave de autenticación, a la que se hace referencia aquí como una clave de enlace K_1 que puede usarse para permitir la subsiguiente autenticación entre los dispositivos 110, 130 (por ejemplo, la clave de enlace en el protocolo BT BR/EDR, como se describe en la sección 4.2 de la Especificación Bluetooth). El emparejamiento inicial puede llevarse a cabo usando una técnica conocida en la técnica, y el emparejamiento inicial puede llevarse a cabo usando medios en banda o medios fuera de banda. El emparejamiento puede ser, opcionalmente, seguido por unión, como se indica en el bloque 320. El proceso de unión puede implicar que el primer dispositivo 110 y el segundo dispositivo 130 almacenen la clave de enlace K_1 para la autenticación del otro dispositivo en posteriores intentos de conexión por el otro dispositivo.

El método 300 continúa con la obtención de un segundo secreto compartido, es decir, una clave de autenticación, entre el primer dispositivo 110 y el segundo dispositivo 130, como se indica en el bloque 330. El segundo secreto compartido se refiere aquí como una clave de enlace predeterminada K_d. La clave de enlace predeterminada obtenida K_d se almacena en el segundo dispositivo 130 y posiblemente en el primer dispositivo 110 para posteriores propósitos de autenticación. El papel de la clave de enlace predeterminada K_d es diferente de la de la clave de enlace K_1 en que la clave de enlace por defecto K_d puede ser posteriormente suministrada a otros dispositivos y puede ser reutilizada (para autenticación) por los dispositivos adicionales, mientras que la clave de enlace K_1 es específica para el par del primer dispositivo 110 y el segundo dispositivo 130. Por lo tanto, la clave de enlace K_1 (y cualquier clave de enlace específica para un cierto par de dispositivos) se refiere aquí como una clave de enlace dedicada, mientras que la clave de enlace predeterminada K_d (y cualquier otra clave de enlace predeterminada) también se puede denominar clave de enlace compartido.

La clave de enlace predeterminada K_d pueden comunicarse adicionalmente a otros dispositivos para facilitar la autenticación automatizada en el establecimiento de conexión posterior con el segundo dispositivo 130 mediante la reutilización de la clave de enlace predeterminada K_d, como se describirá más adelante en este texto con más detalle. Con el fin de asegurar que el emparejamiento y la posible unión entre el primer dispositivo 110 y el segundo dispositivo 130 no se vean comprometidos debido a que cualquiera de los dispositivos adicionales que hacen uso de la clave de enlace por defecto compartida K_d en el subsiguiente establecimiento de conexión y autenticación con el segundo dispositivo 130, la clave de enlace por defecto K_d es, preferentemente, diferente de la clave de enlace K_1.

El primer dispositivo 110 y/o el segundo dispositivo 130 pueden estar dispuestos para obtener la clave de enlace por defecto en una de una pluralidad de maneras. Como algunos ejemplos,

- La clave de enlace predeterminada K_d puede almacenarse previamente en uno del primer dispositivo 110 y el segundo dispositivo 130 y suministrada al otro dispositivo 110, 130;
- La clave de enlace predeterminada K_d puede crearse en uno del primer dispositivo 110 y en el segundo dispositivo 130 (por ejemplo, sobre la base de un indicador asociado al otro dispositivo 110, 130) y se suministra al otro dispositivo 110, 130;
- La clave de enlace predeterminada K_d puede almacenarse previamente o crearse en el dispositivo servidor 170 uno del primer dispositivo 110 y el segundo dispositivo 130 (por ejemplo, sobre la base de un indicador asociado a uno o más del primer dispositivo 110 y el segundo dispositivo 130) y se suministra al primer

dispositivo 110 y/o al segundo dispositivo 130 (y posiblemente además al otro dispositivo 110, 130).

La obtención de la clave de enlace predeterminada K_d y la entrega de la clave de enlace predeterminada K_d desde el dispositivo servidor 170 al primer dispositivo 110 o al segundo dispositivo 130 y desde uno del primer dispositivo 110 y el segundo dispositivo 130 al otro dispositivo 110, 130 puede implicar el uso de un protocolo predefinido de gestión de claves predeterminado diseñado para este fin. Un protocolo de gestión de claves por defecto de este tipo puede, además, permitir el intercambio de información entre los dispositivos implicados con el fin de transmitir y/o recibir información asociada a cualquiera de los dispositivos 110, 130, 170 involucrados y/o un usuario del mismo, por ejemplo, para habilitar la creación de la clave de enlace predeterminada K_d y/u otra información de emparejamiento predeterminada. El protocolo de administración de claves predeterminado puede permitir además un proceso de negociación con respecto al origen y entrega de la clave de enlace predeterminada K_d.

El segundo dispositivo 130 puede estar dispuesto para rechazar la obtención de una nueva clave de enlace predeterminada K_d en caso de que ya haya obtenido una clave de enlace predeterminada y el segundo dispositivo 130 no admita múltiples claves de enlace predeterminadas. En general, el segundo dispositivo 130 puede estar dispuesto para disminuir de obtener otra clave de enlace por defecto K_d en respuesta a haber obtenido ya un número máximo predefinido de claves de enlace predeterminadas, mientras que el segundo dispositivo 130 puede estar dispuesto para continuar con la obtención de otra clave de enlace predeterminada K_d en respuesta a haber obtenido menos que el número máximo predefinido de claves de enlace predeterminadas.

En caso de que la clave de enlace predeterminada K_d no procede del dispositivo servidor 170, el método 300 puede continuar con la entrega de la clave de enlace predeterminada K_d al dispositivo servidor 170 para su posterior entrega a uno o más terceros dispositivos 150, como se indica en el bloque 340. La entrega puede implicar ya sea el primer dispositivo 110 o el segundo dispositivo 130 configurado para entregar la clave de enlace predeterminada obtenida K_d al dispositivo servidor 170. La entrega puede emplear el protocolo de gestión de clave por defecto antes mencionado.

El método 300 continúa con la entrega de la identificación del segundo dispositivo 130 al dispositivo servidor 170 para su posterior entrega a uno o más terceros dispositivos 150, como se indica en el bloque 350. La entrega puede implicar ya sea el primer dispositivo 110 o el segundo dispositivo 130 configurado para entregar una identificación del segundo dispositivo 130 al dispositivo servidor 170. La identificación del segundo dispositivo 130 puede comprender, por ejemplo, una dirección MAC de la porción de comunicación inalámbrica 132 u otra dirección o identificador adecuado asociado al segundo dispositivo 130. Además de esta identificación, también, por ejemplo, una identificación de un usuario del primer dispositivo 110 (por ejemplo, una dirección de correo electrónico, un número de teléfono, una cuenta de usuario, etc.) puede ser entregada al dispositivo servidor 170 y/o al segundo dispositivo 130. Si se proporciona la identificación del usuario del primer dispositivo 110, se puede decir que el usuario identificado está asociado a la clave de enlace predeterminada respectiva K_d (y viceversa). La clave de enlace predeterminada K_d, la identificación del segundo dispositivo 130, posiblemente junto con la identificación del usuario del primer dispositivo 110, puede denominarse información de emparejamiento por defecto.

El método 300 continúa con la entrega de la información de emparejamiento predeterminada al tercer dispositivo 150. Esto implica entregar al menos la clave de enlace predeterminada K_d y la identificación del segundo dispositivo 130 al tercer dispositivo 150, como se indica en el bloque 360. La información proporcionada permite al tercer dispositivo 150 descubrir posteriormente el segundo dispositivo 130 y autenticarse durante un procedimiento de establecimiento de conexión con el segundo dispositivo 130 (como se describirá con más detalle más adelante en este texto).

Una vez que tenga al menos la clave de enlace predeterminada K_d, y la identificación del segundo dispositivo 130 incluida en la información de emparejamiento por defecto en su disposición, el tercer dispositivo 150 puede aplicar esta información para descubrir el segundo dispositivo 130 y autenticarse en el establecimiento de conexión con el segundo dispositivo 130. En paralelo, el segundo dispositivo 130 está habilitado para hacer uso de la clave de enlace por defecto K_d almacenada en el mismo con el fin de autenticar el tercer dispositivo 150 de una manera automatizada, es decir, sin necesidad de acciones del usuario. A este respecto, el segundo dispositivo 130 puede estar habilitado para operar selectivamente la porción de comunicación inalámbrica 132 en uno de una pluralidad de estados predefinidos. Como ejemplo, estos estados operativos pueden comprender uno o más de los siguientes, posiblemente junto con estados operacionales adicionales: un estado en el que la porción de comunicación inalámbrica 132 es conectable pero no detectable por otros dispositivos inalámbricos, un estado en el que la porción de comunicación inalámbrica 132 es Detectable por otros dispositivos inalámbricos y un estado en el que la porción de comunicación inalámbrica 132 está conectada con otro dispositivo inalámbrico.

La figura 4 ilustra un método de ejemplo 400 para facilitar el establecimiento de la conexión entre el segundo dispositivo 130 y el tercer dispositivo 150 haciendo uso de la clave de enlace por defecto K_d para autenticar el tercer dispositivo 150. En particular, la clave de enlace predeterminada K_d es utilizable para autenticación automatizada del tercer dispositivo 150 que es previamente desconocido por el segundo dispositivo 130, por ejemplo, no unido con el segundo dispositivo 130. La autenticación automatizada llevada a cabo en el transcurso del método 400 requiere que el segundo dispositivo 130 tenga el conocimiento de al menos una clave de enlace predeterminada, por

ejemplo, la clave de enlace predeterminada K_d. A este respecto, al menos una clave de enlace por defecto puede almacenarse previamente en la memoria 135 y, por lo tanto, disponible para fines de autenticación en el contexto del establecimiento de asociación y/o conexión a uno o más terceros dispositivos 150. La clave de enlace preestablecida por defecto se puede obtener, por ejemplo, de acuerdo con un procedimiento resumido en lo anterior en el contexto del método 300.

El método 400 comienza desde el segundo dispositivo 130 que opera la porción de comunicación inalámbrica 132 en un estado en el que es conectable pero no detectable por otros dispositivos, como se indica en el bloque 410. A este respecto, para permitir ser conectados por los dispositivos que ya tienen conocimiento de su identidad, el segundo dispositivo 130 puede estar configurado para operar la porción de comunicación inalámbrica 132 en un estado en el que es conectable por otros dispositivos, pero no detectable por otros dispositivos. Como ejemplo, en el marco del protocolo BT BR/EDR esto corresponde a una operación de exploración de página, en la que la porción de comunicación inalámbrica 132 está configurada para explorar mensajes de paginación transmitidos por otros dispositivos.

En paralelo, el tercer dispositivo 150 puede configurarse para hacer que la porción de comunicación inalámbrica 152 solicite conexión con el segundo dispositivo. La petición de conexión puede implicar la transmisión de uno o más mensajes dirigidos a la porción de comunicación inalámbrica 132. Estos mensajes pueden comprender una solicitud de conexión explícita y/o uno o más mensajes que sirven como solicitud(es) de información que permite que el tercer dispositivo 150 establezca conexión con el segundo dispositivo 130. A este respecto, el tercer dispositivo 150 puede estar dispuesto para hacer uso de la identificación del segundo dispositivo 130 obtenida del dispositivo servidor 170 como parte de la información de emparejamiento predeterminada para permitir el direccionamiento de la solicitud de conexión al segundo dispositivo 130. Como ejemplo, en el marco del protocolo BT BR/EDR esto corresponde a la operación de paginación, en la que la porción de comunicación inalámbrica 152 está dispuesta para transmitir uno o más mensajes de paginación dirigidos al segundo dispositivo 130 (transmitiendo paquetes de ID que consisten en o Incluyen un código de acceso a un dispositivo (DAC) de la porción de comunicación inalámbrica 132, DAC que puede derivarse de la dirección MAC de la porción de comunicación inalámbrica 132).

Si bien la porción de comunicación inalámbrica 132 del segundo dispositivo 130 está naturalmente habilitada para recibir solicitudes de conexión (por ejemplo, mensajes de paginación) desde cualquier dispositivo que emplee el protocolo de comunicación soportado, para mayor claridad y brevedad de descripción, a continuación, se describe el funcionamiento a este respecto suponiendo que la fuente de la solicitud de conexión es el tercer dispositivo 150.

El segundo dispositivo 130 puede configurarse para continuar con el procedimiento de asociación y autenticación en respuesta a haber recibido la solicitud de conexión del tercer dispositivo 150, como se indica en el bloque 420. El segundo dispositivo 130 puede estar configurado además para causar, en respuesta a haber recibido la solicitud de conexión desde el tercer dispositivo 150, la porción de comunicación inalámbrica 132 para responder a la petición de conexión transmitiendo uno o más mensajes de respuesta dirigidos al tercer dispositivo 150. Este intercambio de mensajes puede realizarse, por ejemplo, para intercambiar información de sincronización y/u otra información requerida para la configuración de conexión entre los dispositivos 130 y 150. A modo de ejemplo, en el marco del protocolo BT BR/EDR este intercambio de mensajes corresponde a una operación de respuesta de página, en la que el segundo dispositivo 130 responde a mensajes de paginación transmitiendo uno o más paquetes ID y el tercer dispositivo 150 responde además mediante la transmisión de uno o más paquetes de sincronización de salto de frecuencia (FHS) para proporcionar información de establecimiento de conexión.

Cuando el segundo dispositivo 130 ha recibido y posiblemente respondió a la petición de conexión recibida desde el tercer dispositivo 150 y se ha llevado a cabo otro cambio de señalización posiblemente necesario, el método 400 continúa con la verificación de si el segundo dispositivo 130 tiene uno o más enlaces almacenados previamente como se indica en el bloque 430. Las claves de enlace disponibles en el segundo dispositivo 130 pueden incluir una o más claves de enlace dedicadas y/o una o más claves de enlace predeterminadas. Las claves de enlace dedicadas pueden comprender, por ejemplo, la clave de enlace dedicada K_1 descrita en el anterior y/o una clave de enlace dedicada K_3 obtenida o creada en un procedimiento de emparejamiento anterior (y enlace) llevado a cabo entre el segundo dispositivo 130 y el tercer dispositivo 150. Como ejemplo adicional, las claves de enlace almacenadas en el segundo dispositivo 130 pueden comprender la clave de enlace por defecto K_d, que, como se ha descrito anteriormente, puede ser una clave de enlace que se comparte con una serie de dispositivos. A este respecto, el segundo dispositivo 130 puede configurarse para verificar, en respuesta a haber recibido el mensaje o mensajes de búsqueda de otro dispositivo, si el segundo dispositivo 130 tiene una o más claves de enlace almacenadas en el mismo y por lo tanto disponibles para el establecimiento de conexión automática y autenticación del otro dispositivo.

En respuesta a un fallo en la búsqueda de claves de enlace almacenadas previamente en el segundo dispositivo 130, falla el intento de conexión con el tercer dispositivo 150 (bloque 460) y el método 400 vuelve a operar la porción de comunicación inalámbrica 132 en el estado donde es conectable pero no detectable por otros dispositivos (bloque 410). Por el contrario, en respuesta a encontrar al menos una clave de enlace almacenada en el segundo dispositivo 130, el método 400 procede a verificar si cualquiera de las claves de enlace almacenadas previamente es una clave de enlace válida para la fuente del mensaje(s) de paginación, como se indica en el bloque 440. A este respecto, el

segundo dispositivo 130 puede configurarse para verificar, en respuesta a haber encontrado al menos una clave de enlace almacenada previamente, si cualquiera de las claves de enlace almacenadas previamente disponibles es una clave de enlace válida para la fuente del (los) mensaje(s) de paginación. En la técnica se conocen procedimientos de verificación adecuados.

Como ejemplo ilustrativo del procedimiento de verificación para la verificación de la validez de una única clave de enlace almacenada previamente, el segundo dispositivo 130 puede enviar un mensaje que incluye un reto (por ejemplo, un número aleatorio) a la fuente del mensaje o mensajes de búsqueda y el dispositivo de fuente puede calcular una respuesta usando una función predefinida que es una función de al menos el reto y la clave de enlace asociada al segundo dispositivo 130 en el dispositivo de fuente. La fuente puede enviar un mensaje que incluye la respuesta de vuelta al segundo dispositivo 130 y el segundo dispositivo 130 calcula una respuesta de referencia local que aplica la función predefinida para el reto y la clave de enlace bajo verificación. La verificación de la clave de enlace bajo verificación tiene éxito si la respuesta de referencia es igual a la respuesta recibida de la fuente (lo que implica que el segundo dispositivo 130 y la fuente han aplicado claves de enlace idénticas), mientras que la verificación no tiene éxito en caso de que la respuesta recibida de la fuente es diferente de la respuesta de referencia. Como ejemplo, suponiendo que el dispositivo fuente es el tercer dispositivo 150, la verificación tiene éxito, por ejemplo, en el caso de que tanto el segundo dispositivo 130 como el tercer dispositivo 150 apliquen la clave de enlace dedicada K_3 obtenida o creada en un procedimiento de emparejamiento anterior (y enlace) llevado a cabo entre estos dispositivos y en caso de que tanto el segundo dispositivo 130 como el tercer dispositivo 150 apliquen la clave de enlace dedicada K_3.

En el ejemplo anterior, el segundo dispositivo 130 actúa como un verificador mientras que la fuente (por ejemplo, el tercer dispositivo 150) actúa como un reclamante. Como otro ejemplo, el procedimiento de verificación puede llevarse con los roles invertidos, es decir, tal que la fuente actúa como verificador (y por lo tanto envía el reto y verifica la respuesta recibida) mientras que el segundo dispositivo 130 actúa como el reclamante (y por lo tanto computa la respuesta sobre la base del reto recibido).

En el caso de que existan múltiples claves de enlace almacenadas previamente en el segundo dispositivo 130, el procedimiento de ejemplo descrito anteriormente entre el verificador y el solicitante puede ser llevado hasta que se haya encontrado una clave de enlace válida entre las claves de enlace almacenadas previamente en el segundo dispositivo 130 o hasta que se hayan considerado todas las claves de enlace almacenadas previamente disponibles sin encontrar una válida.

Como ejemplo, en el marco del protocolo BT BD/EDR, puede emplearse un procedimiento de verificación posterior al especificado en el Especificación Bluetooth, vol. 2, Parte C, Sección 4.2.

El segundo dispositivo 130 puede estar dispuesto para aplicar un procedimiento de verificación para verificar si cualquiera de las claves de enlace almacenadas previamente es una clave de enlace válida para la fuente de la solicitud de conexión, es decir, para el tercer dispositivo 150 (y/o la porción de comunicación inalámbrica 152 del mismo). El procedimiento de verificación puede considerar todas las claves de enlace almacenadas previamente o un subconjunto limitado de las claves de enlace almacenadas previamente en un orden de preferencia predefinido, de modo que la verificación se complete con éxito - y por lo tanto el tercer dispositivo 150 sea autenticado con éxito - en respuesta a encontrar la primera clave de enlace válida almacenada previamente, mientras se termina la verificación - y por lo tanto falla la autenticación - en respuesta a una falla al encontrar ninguna de las claves de enlace almacenadas previamente consideradas como válidas. La orden de preferencia puede definir que se comprueban primero las claves de enlace dedicadas que se consideran, seguidas por la verificación de las claves de enlace predeterminadas que se consideren. Tal orden de preferencia da como resultado el uso del posible emparejamiento directo y la unión realizados anteriormente con el tercer dispositivo 150 si la correspondiente clave de enlace dedicada (K_3) está disponible y recurriendo a un emparejamiento que se basa en la clave de enlace predeterminada (compartida) K_d en caso de que ninguna clave de enlace dedicada (K_3) que indica el emparejamiento y la unión directa con el tercer dispositivo 150 está disponible.

El procedimiento de verificación puede considerar además la información adicional recibida del tercer dispositivo 150 en la selección de las claves de enlace almacenadas previamente a considerar en el procedimiento de verificación. Como ejemplo, el segundo dispositivo 130 puede recibir la identificación del dispositivo fuente en el curso del intercambio de señalización llevado a cabo como parte del establecimiento de conexión (por ejemplo, en un paquete FHS en el caso de que se aplique el protocolo BT BR/EDR). En dicho escenario, el segundo dispositivo 130 puede considerar primero en el procedimiento de verificación cualesquiera claves de enlace dedicadas almacenadas previamente asociadas al dispositivo de fuente identificado, seguido por la consideración de cualesquiera claves de enlace preestablecidas por defecto si es necesario. Si no están disponibles en el segundo dispositivo 130 claves de enlace dedicadas preestablecidas asociadas al dispositivo de fuente, el procedimiento de verificación puede proceder directamente a la consideración de cualesquiera claves de enlace preestablecidas predeterminadas disponibles.

El procedimiento de verificación puede considerar además la información adicional asociada a la clave de enlace predeterminada K_d, por ejemplo, la identificación del usuario del primer dispositivo 110. Como ejemplo a este

respecto, el segundo dispositivo 130 puede recibir una identificación del usuario desde el tercer dispositivo 150 (por ejemplo, en la solicitud de conexión u otros mensajes que se originan desde el tercer dispositivo 150) y considerar en el procedimiento de verificación solamente la clave(s) almacenada(s) previamente de enlace predeterminada(s) y/o las claves de enlace dedicadas almacenadas previamente asociadas a este usuario identificado.

Consecuentemente, el emparejamiento entre el segundo dispositivo 130 y el tercer dispositivo 150 es exitoso en el caso de que el tercer dispositivo 150 sea autenticado satisfactoriamente como resultado del procedimiento de verificación, como se indica en el bloque 450, y el método 400 puede proceder a operar la porción de comunicación inalámbrica 132 en un estado conectado. Por el contrario, el emparejamiento entre el segundo dispositivo 130 y el tercer dispositivo 150 falla y el intento de emparejamiento es rechazado en caso de que el resultado del procedimiento de verificación indique una falta de autenticación del tercer dispositivo 150, como se indica en el bloque 460 y el método 400 puede volver a operar la porción de comunicación inalámbrica 132 en el estado en el que es conectable pero no puede ser detectado por otros dispositivos (bloque 410). A este respecto, el segundo dispositivo 130 puede estar configurado para operar la porción de comunicación inalámbrica 132 de acuerdo con el resultado del procedimiento de verificación, por ejemplo, para hacer que la porción de comunicación inalámbrica 132 establezca la conexión con el tercer dispositivo 150 o para rechazar el intento de emparejamiento y volver a operar la porción de comunicación inalámbrica 132 en el estado en el que es conectable pero no detectable por otros dispositivos de acuerdo con el resultado.

Un intento fallido de emparejamiento desde el tercer dispositivo 150 debido a una autenticación fallida puede resultar además que el segundo dispositivo 130 prohíba un número predefinido de intentos de emparejamiento posteriores (por ejemplo, uno) o cualquier intento de emparejamiento posterior por el tercer dispositivo 150 en general. Como otro ejemplo, un intento de emparejamiento fallido puede dar como resultado que el segundo dispositivo 130 prohíba un número predefinido de intentos de emparejamiento posteriores (por ejemplo, uno) o cualquier intento de emparejamiento posterior por el tercer dispositivo 150 que se basan en la clave de enlace predeterminada K_d.

Como una alternativa a la autenticación descrita con referencias al método 400, puede aplicarse un procedimiento de emparejamiento 'estándar' que procede del descubrimiento de dispositivo por el tercer dispositivo 130. La figura 5 ilustra un esquema de un procedimiento de ejemplo 500 a este respecto. Como se ha descrito en lo que antecede, el segundo dispositivo 130 puede estar habilitado para operar selectivamente la porción de comunicación inalámbrica 132 en uno de una pluralidad de estados predefinidos, por ejemplo, En uno de los siguientes: un estado en el que la porción de comunicación inalámbrica 132 es conectable pero no detectable por otros dispositivos inalámbricos, un estado en el que la porción de comunicación inalámbrica 132 es detectable por otros dispositivos inalámbricos y un estado en el que la porción de comunicación inalámbrica 132 está conectada con otro dispositivo inalámbrico. En consecuencia, el segundo dispositivo 130 puede estar dispuesto para permitir el funcionamiento selectivo de la porción de comunicación inalámbrica 132 de tal manera que el establecimiento de conexión pueda llevarse a cabo de acuerdo con el método 400 o según el método 500, dependiendo del estado de funcionamiento.

El método 500 comienza desde el segundo dispositivo 130 que opera la porción de comunicación inalámbrica 132 en un estado en el que es detectable por otros dispositivos, como se indica en el bloque 510. Como ejemplo, en el marco del protocolo BT BR/EDR esto corresponde a una operación de exploración de consulta, en la que la porción de comunicación inalámbrica 132 está configurada para explorar mensajes de consulta transmitidos por otros dispositivos.

En paralelo, el tercer dispositivo 150 puede ser accionado en un estado de descubrimiento de dispositivo para encontrar otros dispositivos. A este respecto, el tercer dispositivo 150 puede estar dispuesto para hacer que la porción de comunicación inalámbrica 152 transmita uno o más mensajes de consulta. El segundo dispositivo 130 puede estar configurado para continuar con el procedimiento de descubrimiento de dispositivos en respuesta a haber detectado la presencia del tercer dispositivo 150 (bloque 515), por ejemplo, en respuesta a la detección de los mensajes de consulta transmitidos desde el tercer dispositivo 150. El segundo dispositivo 130 puede configurarse adicionalmente para causar, en respuesta a haber detectado mensajes de consulta, la porción de comunicación inalámbrica 132 para responder al mensaje o mensajes de consulta transmitiendo uno o más mensajes de respuesta de consulta. Posteriormente, cada uno del segundo dispositivo 130 y el tercer dispositivo 150 pueden transmitir y/o recibir uno o más mensajes con el fin de intercambiar información de sincronización y/u otra información requerida para la configuración de la conexión. Como ejemplo, en el marco del protocolo BT BR/EDR, la operación correspondiente al bloque 515 puede corresponder a una operación de respuesta de consulta, en la que el segundo dispositivo 130 responde a paquetes de ID transmitidos como mensaje(s) de búsqueda desde el tercer dispositivo 150 mediante la transmisión de uno o más paquetes FHS para proporcionar información de configuración de conexión.

Después del proceso de investigación, el método 500 continúa realizando un procedimiento de búsqueda para facilitar la configuración y establecimiento de la conexión entre el segundo dispositivo 130 y el tercer dispositivo 150, como se indica en el bloque 520. Para habilitar el establecimiento de conexión, el segundo dispositivo 130 puede estar dispuesto para hacer que la porción de comunicación inalámbrica funcione en el estado en el que es conectable pero no detectable por otros dispositivos (por ejemplo, la operación de exploración de página del protocolo BT BR/EDR) después de finalizado el proceso de investigación. El funcionamiento del bloque 520

corresponde a la operación descrita en el contexto de los bloques 410 y 420 del método 400 con la excepción de que aquí la identidad del segundo dispositivo 130 se obtiene mediante el procedimiento de consulta (bloques 510 y 515) en lugar de hacer uso de la información de emparejamiento predeterminada obtenida del dispositivo servidor 170.

Después del procedimiento de búsqueda, el método 500 procede a verificar si el segundo dispositivo 130 tiene una o más claves de enlace almacenadas previamente, como se indica en el bloque 530. La operación del bloque 530 corresponde a la del bloque 430 del método 400 con la excepción de que aquí solamente las claves de enlace dedicadas (por ejemplo, K_1 y K_3) mientras que la clave de enlace predeterminada K_d y/o cualquier otra clave de enlace predeterminada adicional se excluyen de la consideración.

En respuesta a una falla en la búsqueda de claves de enlace pre-almacenadas (dedicadas) disponibles en el segundo dispositivo 130, el segundo dispositivo 130 procede a realizar un procedimiento de emparejamiento 'estándar' para crear/obtener una clave de enlace (dedicada) para el par del segundo dispositivo 130 y el tercer dispositivo 150, como se indica en el bloque 560. Por el contrario, el contraste 500, en respuesta a encontrar al menos una clave de enlace almacenada previamente (dedicada) para estar disponible en el segundo dispositivo 130, el método 500 procede a verificar si cualquiera de las claves de enlace almacenadas previamente es una clave de enlace válida para la fuente de los mensajes de búsqueda, tal como se indica en el bloque 540. En general, el funcionamiento del bloque 540 corresponde al del bloque 440 del método 400 con la excepción de que solo se consideran en el procedimiento de verificación las claves de enlace dedicadas.

En consecuencia, el emparejamiento entre el segundo dispositivo 130 y el tercer dispositivo 150 tiene éxito en caso de que el tercer dispositivo 150 sea autenticado satisfactoriamente como resultado del procedimiento de verificación (del bloque 540), como se indica en el bloque 550, y el método 500 puede continuar para operar la porción de comunicación inalámbrica 132 en un estado conectado. Por el contrario, en respuesta a un fallo en la autenticación del tercer dispositivo 150 que utiliza cualquiera de las claves de enlace preestablecidas (dedicadas) disponibles en el segundo dispositivo 130, el segundo dispositivo 130 procede a llevar a cabo el procedimiento de emparejamiento 'estándar' para crear/obtener una clave de enlace (dedicada) para el par del segundo dispositivo 130 y el tercer dispositivo 150 (bloque 560).

Después de haber realizado un apareamiento inicial y una posible unión con el primer dispositivo 110, como ejemplo, el segundo dispositivo 130 puede estar dispuesto para utilizar exclusivamente la clave de enlace por defecto K_d para otros intentos de conexión por cualquier tercer dispositivo 150 (por ejemplo, de acuerdo con el método 400). Tal aproximación sirve para facilitar que el segundo dispositivo 130 empareje y autenticando automáticamente solo aquellos dispositivos que han obtenido la clave de enlace predeterminada desde el dispositivo servidor 170, normalmente con dispositivos de un solo usuario que desea hacer uso del segundo dispositivo 130 (también) con uno o más terceros dispositivos 150.

Como otro ejemplo, el segundo dispositivo 130 puede estar dispuesto para hacer uso selectivamente de la clave de enlace por defecto K_d (por ejemplo, de acuerdo con el método 400) o un procedimiento de asociación y autenticación "estándar" (por ejemplo, de acuerdo con el método 500). La selección se puede realizar, por ejemplo, a través de la interfaz de usuario del segundo dispositivo 130. A este respecto, una selección que hace que el segundo dispositivo 130 accione la porción de comunicación inalámbrica 132 en el estado en el que es conectable pero no detectable por otros dispositivos puede dar lugar a emparejamiento y autenticación automatizados basándose en la clave de enlace predeterminada K_d, mientras que una selección que hace que el segundo dispositivo 130 accione la porción de comunicación inalámbrica 132 en el estado donde es detectable por otros dispositivos da como resultado el uso del procedimiento de emparejamiento y autenticación "estándar".

Haciendo referencia de nuevo a los componentes del primer dispositivo 110, el segundo dispositivo 130 y el tercer dispositivo 150 descrito en lo anterior, el procesador 116 está configurado para leer y escribir en la memoria 115, el procesador 136 está configurado para leer y escribir en la memoria 135 y el procesador 156 están configurados para leer y escribir en la memoria 155. Aunque el procesador 116, 136, 156 se describe como un componente único, el procesador 116, 136, 156 puede ser implementado como uno o más componentes separados. De forma similar, aunque la memoria 115, 135, 155 se describe como un componente único, la memoria 115, 135, 155 puede ser implementada como uno o más componentes separados, algunos o todos los cuales pueden ser integrados/extraíbles y/o pueden proporcionar almacenamiento permanente/semipermanente/dinámico/en caché.

La memoria 115 puede almacenar el programa informático 117 que comprende instrucciones ejecutables por ordenador que controlan el funcionamiento del aparato 110 cuando se cargan en el procesador 116. Como ejemplo, el programa informático 117 puede incluir una o más secuencias de una o más instrucciones. El programa informático 117 puede proporcionarse como un código de programa de ordenador. El procesador 116 es capaz de cargar y ejecutar el programa informático 117 leyendo una o más secuencias de una o más instrucciones incluidas en ella desde la memoria 115. Una o más secuencias de una o más instrucciones pueden estar configuradas para, cuando son ejecutadas por el procesador 116, hacer que el aparato 110 lleve a cabo operaciones, procedimientos y/o funciones descritos en lo anterior en el contexto del primer dispositivo 110. Por tanto, el aparato 110 puede comprender al menos un procesador 116 y al menos una memoria 115 que incluye un código de programa de

ordenador para uno o más programas, al menos una memoria 115 y el código de programa de ordenador configurado para, con al menos un procesador 116, Hacen que el aparato 110 realice operaciones, procedimientos y/o funciones descritos en lo anterior en el contexto del primer dispositivo 110. Consideraciones similares son igualmente válidas para los componentes 13x correspondientes del segundo dispositivo 130 y para los componentes correspondientes 15x del tercer dispositivo 150.

Cada uno de los programas informáticos 117, 137, 157 puede proporcionarse, por ejemplo, como un producto de programa de ordenador respectivo que comprende al menos un medio no transitorio legible por ordenador que tiene un código de programa almacenado en él, el código de programa, cuando es ejecutado por el dispositivo o aparato respectivo 110, 130, 150, hace que el aparato realice al menos operaciones, procedimientos y/o funciones descritos anteriormente en el contexto del dispositivo respectivo 110, 130, 150.

El medio no transitorio legible por ordenador puede comprender un dispositivo de memoria o un medio de grabación tal como un CD-ROM, un DVD, un disco Blu-ray u otro artículo de fabricación que incorpore de manera tangible el programa informático. Como otro ejemplo, el programa de ordenador puede proporcionarse como una señal configurada para transferir fiablemente el programa de ordenador.

La referencia a un procesador no debe entenderse que abarca solamente procesadores programables, sino también circuitos dedicados tales como matrices de puertas programables por campo (FPGA), circuitos específicos de aplicación (ASIC), procesadores de señales, etc.

REIVINDICACIONES

1. Un aparato (130) para comunicación inalámbrica, comprendiendo el aparato (130)
medios para crear, en un procedimiento de emparejamiento con un primer dispositivo inalámbrico (110), una primera clave de autenticación dedicada a autenticar el primer dispositivo inalámbrico (110);
medios para recibir, en un procedimiento con el primer dispositivo emparejado (110), una primera clave de autenticación por defecto para autenticar un dispositivo inalámbrico que no está emparejado con el aparato (130),
medios para almacenar al menos dicha primera clave de autenticación por defecto para autenticar un dispositivo inalámbrico que no está emparejado con el aparato (130);
medios para operar selectivamente el aparato (130) en uno de estados predefinidos, comprendiendo dichos estados al menos un primer estado, en el que el aparato (130) puede conectarse, pero no puede ser detectado por otros dispositivos inalámbricos;
medios para recibir solicitudes de conexión de otros dispositivos inalámbricos; medios que responden a la recepción, cuando el aparato (130) es accionado en dicho primer estado, una petición de conexión de un segundo dispositivo inalámbrico (150), que no está emparejado con el aparato (130), para verificar si dicha primera clave de autenticación predeterminada es una clave de autenticación válida para dicho segundo dispositivo inalámbrico (150); y
medios, que responden a haber encontrado dicha primera clave de autenticación por defecto como una clave de autenticación válida para dicho segundo dispositivo inalámbrico (150), con el fin de establecer una conexión autenticada con dicho segundo dispositivo inalámbrico (150).

2. Un aparato (130) según la reivindicación 1, que comprende además medios para obtener dicha primera clave de autenticación predeterminada, utilizando un procedimiento de negociación de clave con el primer dispositivo inalámbrico (110), que está emparejado con el aparato (130).

3. Un aparato (130) según las reivindicaciones 1 o 2,
en donde dicha primera clave de autenticación predeterminada está asociada a un usuario predefinido respectivo;
en donde dicha solicitud de conexión comprende una identificación de un usuario; y
en donde dichos medios para verificar están dispuestos para considerar solamente aquellas claves de autenticación predeterminadas que están asociadas al usuario identificado en la petición de conexión.

4. Un aparato (130) según cualquiera de las reivindicaciones 1 a 3, dispuesto para aplicar un protocolo de Bluetooth de tasa básica/tasa de datos mejorada.

5. Un aparato (130) según la reivindicación 4, en el que
dicho primer estado comprende un subestado de exploración de página Bluetooth y;
dicha petición de conexión comprende uno o más mensajes de la página Bluetooth dirigidos al aparato.

6. Un aparato (130) según cualquiera de las reivindicaciones 1 a 3,
en donde dichos estados predefinidos comprenden además un segundo estado, en el que el aparato (130) puede ser detectado por otros dispositivos inalámbricos; y
en donde el aparato (130) comprende además medios, en respuesta a la recepción, cuando el aparato es operado en dicho segundo estado, de una o más solicitudes de un dispositivo inalámbrico adicional, que no está emparejado con el aparato (130), para obtener una autenticación dedicada respectiva con el fin de establecer el emparejamiento con dicho dispositivo inalámbrico adicional.

7. Un aparato (130) según la reivindicación 6, en el que dichos medios para obtener la clave de autenticación dedicada respectiva comprenden
medios, que responden a la recepción, cuando el aparato (130) es operado en dicho segundo estado, de uno o más mensajes de consulta desde dicho dispositivo inalámbrico adicional, para transmitir uno o más mensajes de respuesta de solicitud, que comprenden información que permite el establecimiento de conexión con el aparato (130); y
medios, que responden a recibir una solicitud de conexión desde dicho dispositivo inalámbrico adicional, para obtener la clave de autenticación dedicada respectiva, con el fin de establecer el emparejamiento con dicho dispositivo inalámbrico adicional.

8. Un aparato (130) según las reivindicaciones 6 o 7, dispuesto para aplicar un protocolo de Bluetooth de tasa básica/tasa de datos mejorada.

9. Un aparato (130) según la reivindicación 8, en el que
dicho primer estado comprende un subestado de exploración de página Bluetooth;
dicho segundo estado comprende un subestado de exploración de consulta de Bluetooth; y
dicha petición de conexión comprende uno o más mensajes de página Bluetooth dirigidos al aparato.

10. Un método (400) en un aparato (130) para comunicación inalámbrica, que comprende
crear, en un procedimiento de emparejamiento con un primer dispositivo inalámbrico (110), una primera clave de

autenticación dedicada a autenticar el primer dispositivo inalámbrico (110);
recibir, en un procedimiento con el primer dispositivo emparejado (110), una primera clave de autenticación por defecto para autenticar un dispositivo inalámbrico que no está emparejado con el aparato (130),
almacenar al menos dicha primera clave de autenticación por defecto para autenticar un dispositivo inalámbrico que no está emparejado con el aparato (130);
operar selectivamente (410) el aparato (130) en uno de los estados predefinidos, comprendiendo dichos estados al menos un primer estado, en el que el aparato (130) puede conectarse, pero no puede ser detectado por otros dispositivos inalámbricos;
en respuesta a haber recibido (420), una solicitud de conexión desde un segundo dispositivo inalámbrico (150), que no está emparejado con el aparato (130), cuando el aparato (130) es operado en dicho primer estado, verificar (430, 440) si dicha primera clave de autenticación predeterminada es una clave de autenticación válida para dicho segundo dispositivo inalámbrico (150); y
en respuesta a haber encontrado dicha primera clave de autenticación por defecto como una clave de autenticación válida para dicho segundo dispositivo inalámbrico (150), establecer una conexión autenticada (450) con dicho segundo dispositivo inalámbrico (150).

11. Un método (400) según la reivindicación 10, que comprende, además
obtener dicha primera clave de autenticación por defecto utilizando un procedimiento de negociación de claves con el primer dispositivo inalámbrico (110), que está emparejado con el aparato (130).

12. Un método (400) según las reivindicaciones 10 u 11,
en donde dicha primera clave de autenticación por defecto está asociada a un usuario predefinido respectivo;
en donde dicha solicitud de conexión comprende una identificación de un usuario; y
en donde dicha verificación comprende verificar solamente aquellas claves de autenticación por defecto que están asociadas al usuario identificado en la solicitud de conexión.

13. Un método (400) según cualquiera de las reivindicaciones 10 a 12, en donde dichos estados predefinidos comprenden además un segundo estado, en el que el aparato (130) es detectable por otros dispositivos inalámbricos, comprendiendo además el método,
en respuesta a la recepción, cuando el aparato (130) es operado en dicho segundo estado, de una o más solicitudes de un dispositivo inalámbrico adicional, que no está emparejado con el aparato (130), la obtención de una clave de autenticación dedicada respectiva con el fin de establecer el emparejamiento con dicho otro dispositivo inalámbrico.

14. Un método (400) según cualquiera de las reivindicaciones 10 a 13, en donde dicho aparato aplica un protocolo de Bluetooth de tasa básica/tasa de datos mejorada.

15. Un programa de ordenador (137), que comprende un código de programa legible por ordenador, configurado para causar la realización del método de cualquiera de las reivindicaciones 10 a 14, cuando dicho código de programa es ejecutado en un aparato de cálculo (130).

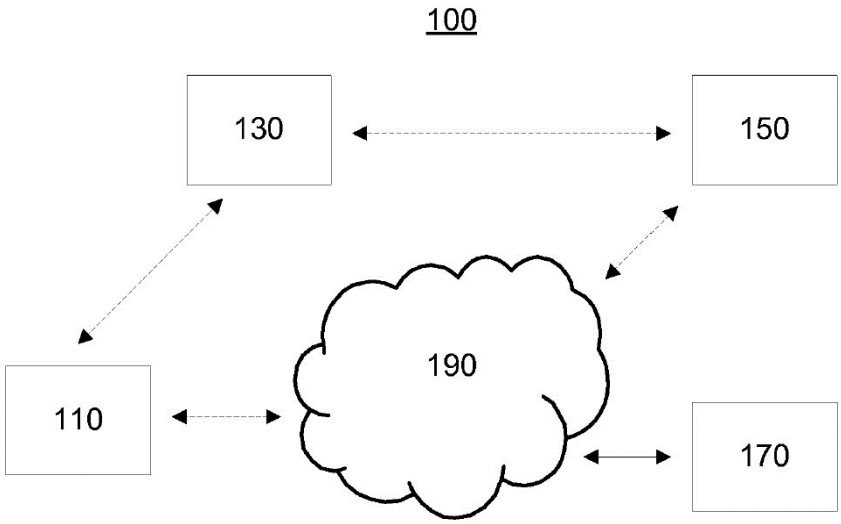

Figura 1

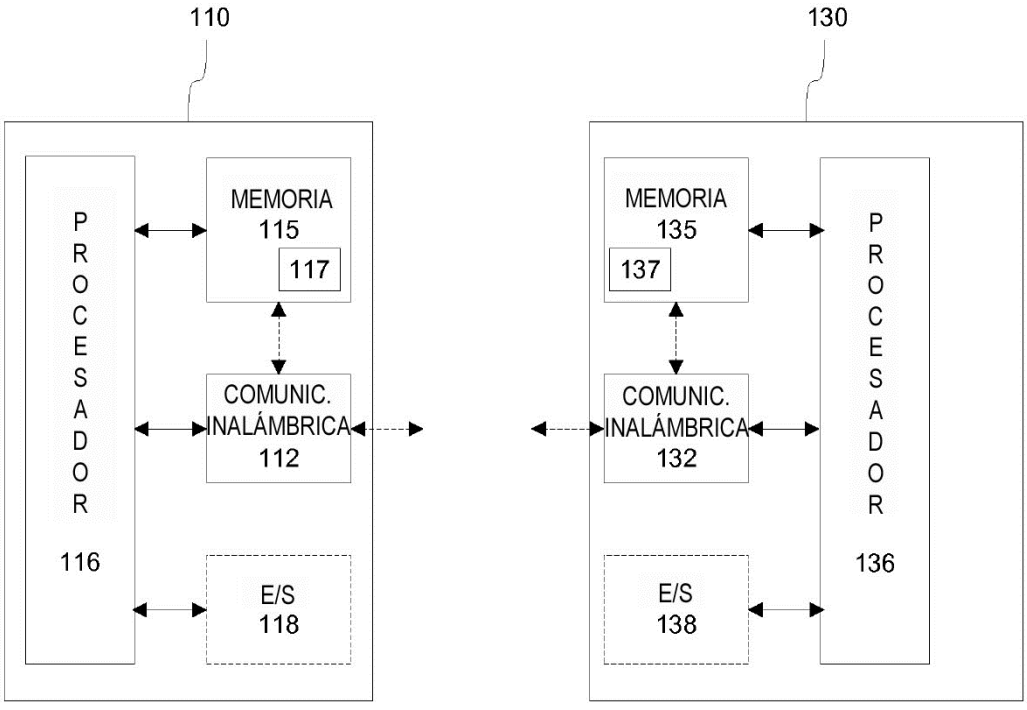

Figura 2a

Figura 2b

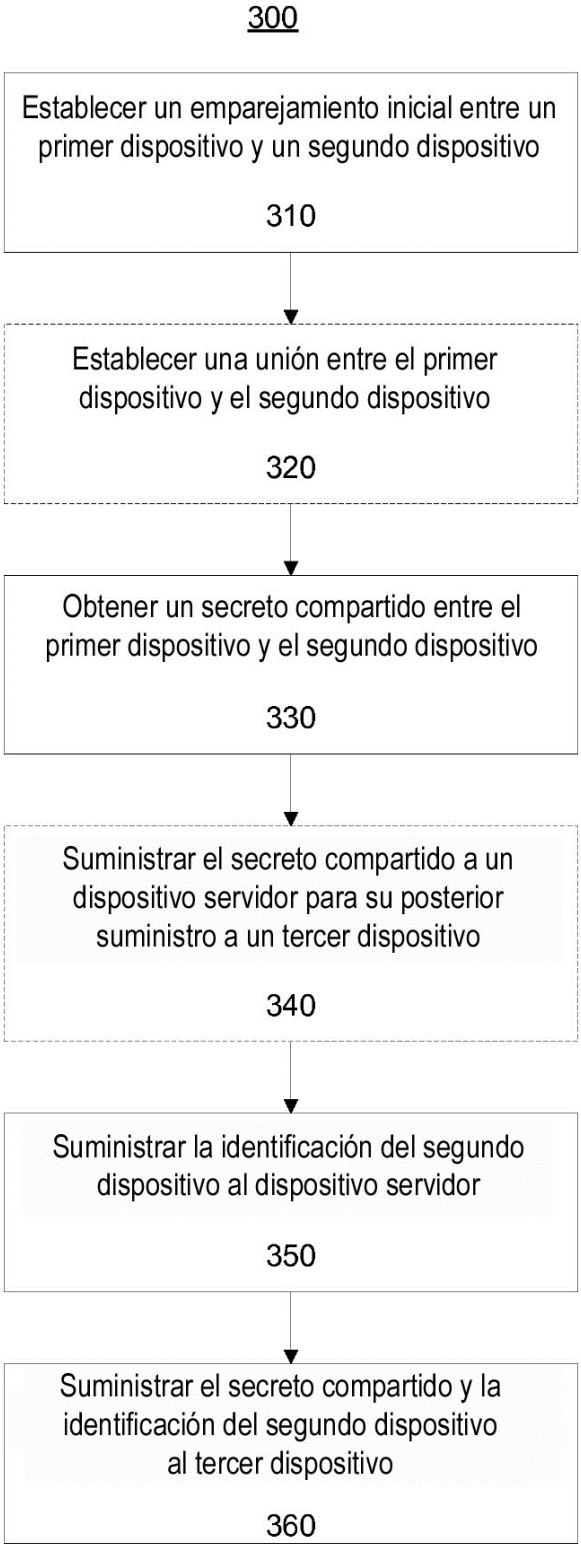
300
Establecer un emparejamiento inicial entre un primer dispositivo y un segundo dispositivo
310
Establecer una unión entre el primer dispositivo y el segundo dispositivo
320
Obtener un secreto compartido entre el primer dispositivo y el segundo dispositivo
330
Suministrar el secreto compartido a un dispositivo servidor para su posterior suministro a un tercer dispositivo
340
Suministrar la identificación del segundo dispositivo al dispositivo servidor
350
Suministrar el secreto compartido y la identificación del segundo dispositivo al tercer dispositivo
360

Figura 3

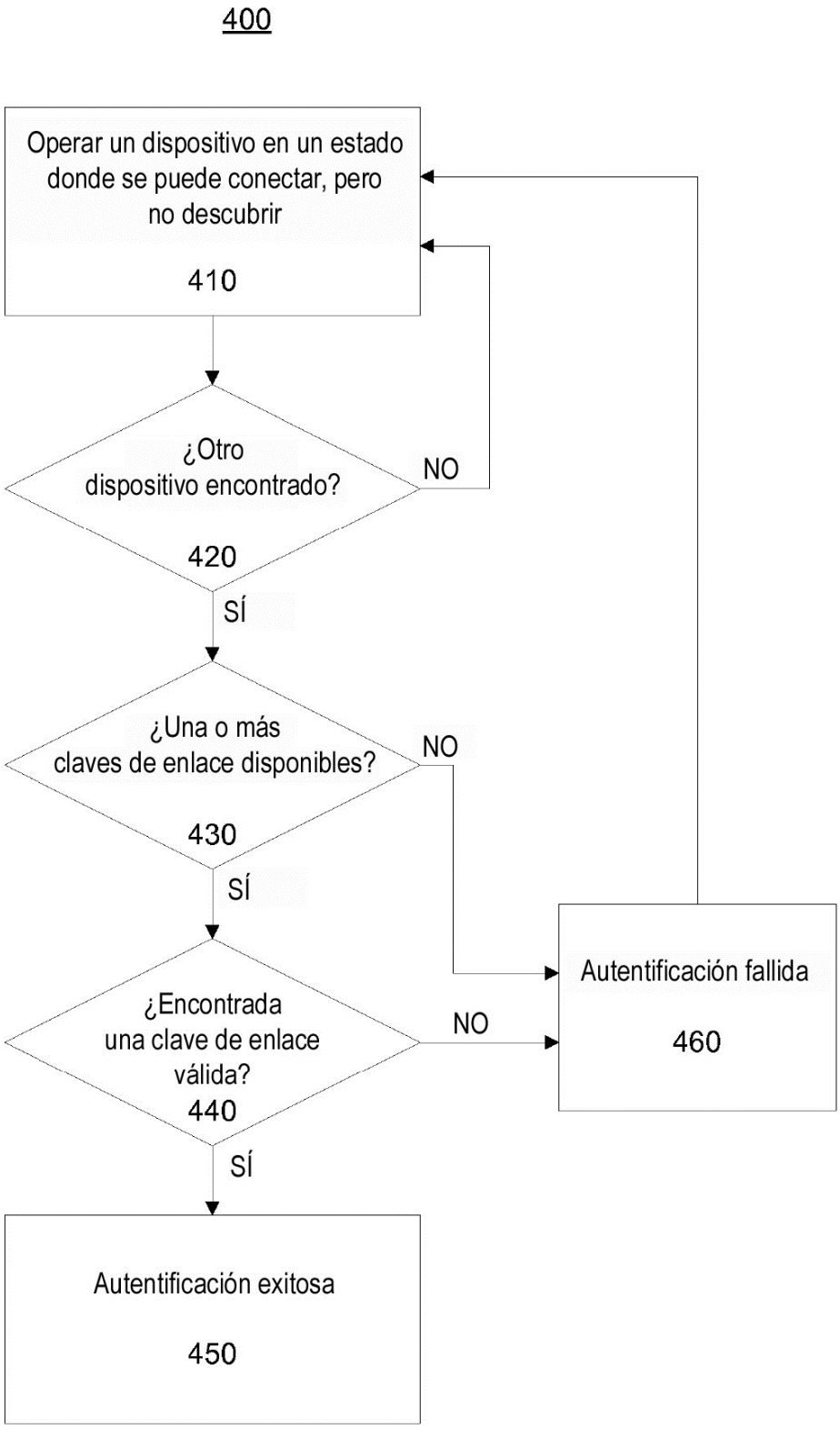
400
Operar un dispositivo en un estado donde se puede conectar, pero no descubrir
410
¿Otro dispositivo encontrado?
420
NO
SÍ
¿Una o más claves de enlace disponibles?
430
NO
SÍ
¿Encontrada una clave de enlace válida?
440
NO
SÍ
Autentificación fallida
460
Autentificación exitosa
450

Figura 4

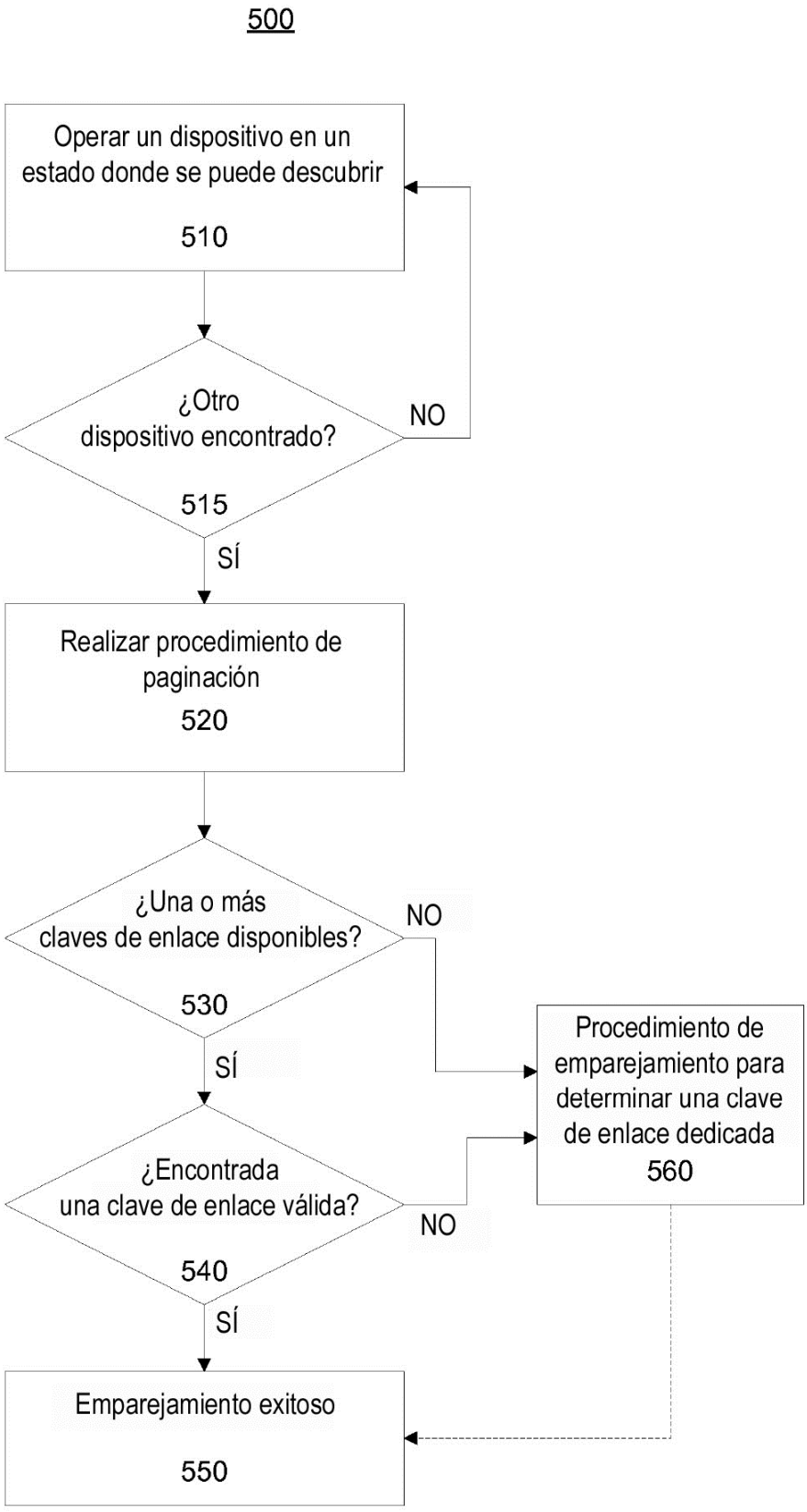
500
Operar un dispositivo en un estado donde se puede descubrir
510
¿Otro dispositivo encontrado?
515
NO
SÍ
Realizar procedimiento de paginación
520
¿Una o más claves de enlace disponibles?
530
NO
SÍ
¿Encontrada una clave de enlace válida?
540
NO
SÍ
Procedimiento de emparejamiento para determinar una clave de enlace dedicada
560
Emparejamiento exitoso
550

Figura 5