(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 659 639**

(51) Int. CI.:

H04L 29/06 (2006.01)
H04W 12/06 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **09.02.2015 PCT/US2015/014992**

(87) Fecha y número de publicación internacional: **13.08.2015 WO15120373**

(96) Fecha de presentación y número de la solicitud europea: **09.02.2015 E 15708365 (0)**

(97) Fecha y número de publicación de la concesión europea: **06.12.2017 EP 3105904**

(54) Título: **Aprovisionamiento de dispositivos asistido en una red**

(30) Prioridad:

10.02.2014 US 201461937891 P
14.05.2014 US 201461996812 P
06.02.2015 US 201514616551

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
16.03.2018

(73) Titular/es:

QUALCOMM INCORPORATED (100.0%)
Attn: International IP Administration, 5775 Morehouse Drive
San Diego, CA 92121, US

(72) Inventor/es:

BENOIT, OLIVIER JEAN;
MALINEN, JOUNI KALEVI y
TINNAKORNSRISUPHAP, PEERAPOL

(74) Agente/Representante:

FORTEA LAGUNA, Juan José

DESCRIPCIÓN

Aprovisionamiento de dispositivos asistido en una red

CAMPO TÉCNICO

[1] Los modos de realización de la presente divulgación se refieren en general al campo de los sistemas de comunicación y, más en particular, al aprovisionamiento de dispositivos en una red de comunicación.

ANTECEDENTES

[2] En muchos sistemas de comunicación (por ejemplo, sistemas de comunicación por satélite, sistemas de comunicación inalámbrica, sistemas de comunicación por línea eléctrica (PLC), sistemas de comunicación por cable coaxial, sistemas de línea telefónica, etc.), una red comprende unos dispositivos que se comunican entre sí a través de un medio de comunicación. Típicamente, a un dispositivo se le debe conceder acceso a la red antes de que el dispositivo pueda comunicarse a través del medio de comunicación. El proceso de concesión de acceso puede denominarse aprovisionamiento de dispositivos y puede incluir operaciones para asociación, registro, autenticación y/u otras operaciones.

[3] Sin embargo, el aprovisionamiento de un nuevo dispositivo para una red puede ser técnicamente complicado o difícil para un usuario. Por ejemplo, un nuevo dispositivo puede necesitar registrarse y/o autenticarse en un dispositivo de red (tal como un punto de acceso) para obtener acceso a recursos de red disponibles a través del dispositivo de red. En los sistemas de comunicación tradicionales, el procedimiento de registro puede usar credenciales de seguridad proporcionadas por un usuario a fin de controlar el acceso e impedir el uso no autorizado. Las etapas de registro típicas pueden incluir la introducción de códigos u otra información por parte del usuario cuando el dispositivo cliente se sitúa dentro del alcance de comunicación del dispositivo de red. Sin embargo, estas etapas de configuración pueden parecer demasiado complicadas para algunos usuarios y pueden desalentar el uso de redes y sus recursos completamente.

[4] Además, algunos dispositivos pueden considerarse dispositivos "sin pantalla". Los dispositivos sin pantalla son dispositivos que no tienen una interfaz gráfica de usuario. Ejemplos de dispositivos sin pantalla pueden incluir sensores, bombillas, cámaras, accionadores, aparatos eléctricos, controladores de juegos, equipos de audio u otros dispositivos de comunicación que son capaces de comunicarse a través de la red de comunicación, pero que pueden no tener una interfaz gráfica de usuario debido a limitaciones comerciales o técnicas. La configuración de red inicial de un dispositivo sin pantalla puede ser difícil debido a la falta de una interfaz gráfica de usuario.

[5] La simplificación del aprovisionamiento de dispositivos puede mejorar la experiencia del usuario y fomentar la adopción de más tipos de dispositivos en un sistema de comunicación. En el documento US 2013/0223279 A1 se proporciona un ejemplo del uso de un dispositivo móvil como dispositivo configurador en la técnica anterior.

SUMARIO

[6] La presente divulgación describe diversos modos de realización del aprovisionamiento de dispositivos para facilitar el registro de un dispositivo que se introduce en una red. El aprovisionamiento de dispositivos se puede mejorar utilizando conceptos de criptografía de claves públicas, en la cual las claves públicas se intercambian entre dispositivos utilizando un protocolo de aprovisionamiento de dispositivos. El protocolo de aprovisionamiento de dispositivos puede ser directamente entre dos dispositivos, o puede implicar un tercer dispositivo denominado dispositivo configurador.

[7] El dispositivo configurador puede servir como un intermediario entre un nuevo dispositivo cliente y un dispositivo de red. Por ejemplo, un dispositivo configurador que tiene una relación de confianza con el dispositivo de red puede facilitar un intercambio de claves públicas entre el dispositivo cliente y el dispositivo de red. La relación de confianza puede establecerse usando una comunicación fuera de banda. El registro del nuevo dispositivo cliente puede ser asistido mediante la compartición de una o más claves públicas a través de un canal fuera de banda fiable con el dispositivo configurador. La invención se define mediante las reivindicaciones independientes. Se definen modos de realización adicionales mediante las reivindicaciones dependientes.

BREVE DESCRIPCIÓN DE LOS DIBUJOS

[8] La presente divulgación se podrá comprender mejor, y numerosos objetivos, características y ventajas resultarán evidentes a los expertos en la materia haciendo referencia a los dibujos adjuntos.

La **figura 1** es un diagrama conceptual que introduce conceptos de aprovisionamiento de dispositivos asistido (por ejemplo, registro, configuración y/o autenticación), de acuerdo con un modo de realización de la presente divulgación;

la **figura 2** es un diagrama de bloques de ejemplo que ilustra diversas funciones de compartición de claves, de acuerdo con un modo de realización de la presente divulgación;

la **figura 3** es un diagrama de flujo que ilustra operaciones realizadas por un dispositivo configurador, de acuerdo con un modo de realización de la presente divulgación;

la **figura 4** es un diagrama de flujo de mensajes que ilustra un ejemplo de aprovisionamiento de dispositivos asistido mediante un dispositivo configurador para proporcionar una clave pública de cliente a un dispositivo de red, de acuerdo con modos de realización de la presente divulgación;

la **figura 5** es un diagrama de flujo de mensajes que ilustra un ejemplo de aprovisionamiento de dispositivos asistido en el que un dispositivo cliente supervisa un canal predeterminado, de acuerdo con modos de realización de la presente divulgación;

la **figura 6** es un diagrama de flujo de mensajes que ilustra un ejemplo de aprovisionamiento de dispositivos asistido en el que un dispositivo configurador proporciona una clave de registro a un dispositivo cliente, de acuerdo con modos de realización de la presente divulgación;

la **figura 7** es un diagrama de proceso de mensajes que ilustra un dispositivo configurador y un dispositivo de red que establecen una relación de confianza, de acuerdo con un modo de realización de la presente divulgación;

la **figura 8** es un diagrama de proceso de mensajes que ilustra un dispositivo cliente y un dispositivo de red que establecen una conexión, de acuerdo con un modo de realización de la presente divulgación;

la **figura 9** es un diagrama de proceso de mensajes que ilustra un servicio configurador fiable basado en la nube para el aprovisionamiento de dispositivos asistido, de acuerdo con un modo de realización de la presente divulgación;

la **figura 10** es otro diagrama de proceso de mensajes que ilustra un servicio configurador fiable basado en la nube que usa certificados, de acuerdo con un modo de realización de la presente divulgación;

la **figura 11** es un diagrama de proceso de mensajes que ilustra un punto de acceso que actúa como servicio configurador para facilitar una conexión inalámbrica de igual a igual, de acuerdo con un modo de realización de la presente divulgación;

la **figura 12** es un diagrama de proceso de mensajes que ilustra la agregación de un segundo dispositivo configurador, de acuerdo con un modo de realización de la presente divulgación;

la **figura 13** es un diagrama conceptual que ilustra listas de claves públicas, de acuerdo con un modo de realización de la presente divulgación; y

la **figura 14** es un diagrama de bloques de ejemplo que ilustra un dispositivo capaz de implementar diversos modos de realización de la presente divulgación.

DESCRIPCIÓN DEL (DE LOS) MODO(S) DE REALIZACIÓN

[9] La siguiente descripción incluye sistemas, procedimientos, técnicas, secuencias de instrucciones y productos de programa informático a modo de ejemplo que representan técnicas de la presente divulgación. Sin embargo, debe entenderse que los modos de realización descritos pueden llevarse a la práctica sin estos detalles específicos. Por ejemplo, aunque los ejemplos descritos en el presente documento se refieren al registro en una red de área local inalámbrica (WLAN), los modos de realización no están limitados de esta manera. En otros modos de realización, dispositivos cliente pueden implementar el aprovisionamiento de dispositivos en otras redes de comunicación de medio compartido adecuadas, tales como comunicaciones de línea eléctrica (PLC), redes coaxiales y/o redes de área local de línea telefónica, etc. En algunos casos, instancias de instrucciones, protocolos, estructuras y técnicas que son bien conocidos no se han mostrado con todo detalle a fin de no ofuscar la descripción.

[10] Los modos de realización de la presente divulgación pueden facilitar el aprovisionamiento de dispositivos de un dispositivo cliente con un dispositivo de red de una red de comunicación. El aprovisionamiento de dispositivos puede permitir que el dispositivo cliente obtenga acceso a través del dispositivo de red a otros dispositivos o recursos de red, tales como memorias de datos, impresoras, recursos basados en la nube y/o acceso a Internet, etc. En la presente divulgación, los términos registro, registrar, etc., se usan para referirse, de forma intercambiable, al aprovisionamiento de dispositivos.

[11] En un modo de realización, un dispositivo configurador puede obtener una clave pública de cliente asociada con el dispositivo cliente y enviar la clave pública de cliente al dispositivo de red. El dispositivo de red puede usar la

clave pública de cliente en un proceso de registro entre el dispositivo de red y el dispositivo cliente. Una vez terminado el proceso de registro, el dispositivo cliente puede configurarse para su uso con el dispositivo de red, tal como para obtener acceso a otros recursos de red. También se puede realizar una autenticación adicional como resultado del proceso de registro satisfactorio.

[12] En un modo de realización, el dispositivo de red puede usar la clave pública de cliente para registrar el dispositivo cliente sin compartir (por ejemplo, transmitir) la clave pública de cliente a través de un canal de comunicación entre el dispositivo de red y el dispositivo cliente. Por ejemplo, el dispositivo de red puede usar la clave pública de cliente para generar una clave compartida entre el dispositivo de red y el dispositivo cliente. La clave compartida puede proporcionarse al dispositivo cliente utilizando un protocolo de registro en el que se intercambian claves públicas y cada uno del dispositivo cliente y el dispositivo de red determinan localmente la clave compartida sin transmitir la clave compartida a través del medio de comunicación. El protocolo de registro que se usa puede incluir operaciones basadas, al menos en parte, en el protocolo Diffie-Hellman, la Autenticación simultánea de iguales (SAE), la Configuración Wi-Fi protegida (WPS) y/o cualquier otro protocolo de establecimiento de claves técnicamente viable que use las claves públicas/privadas de cliente y las claves públicas/privadas de red. De esta manera, el permiso para obtener acceso al dispositivo de red puede ser transparente para el usuario del dispositivo cliente, por ejemplo, sin que el usuario tenga que realizar acciones tales como introducir códigos o contraseñas.

[13] La clave pública de cliente se puede determinar y proporcionar al dispositivo de red a través de un dispositivo fiable, tal como un dispositivo configurador. El dispositivo configurador puede estar coubicado con el dispositivo de red, o puede estar separado. El dispositivo configurador puede ser un dispositivo de usuario, tal como un teléfono inteligente, que establece una relación de confianza con el dispositivo de red, tal como un punto de acceso. En algunos modos de realización, el dispositivo configurador puede tener proximidad, o confianza, en relación con el dispositivo cliente. Por ejemplo, el dispositivo configurador puede obtener la clave pública de cliente utilizando una comunicación fuera de banda directamente con el cliente. El uso de una comunicación fuera de banda puede ayudar al evitar posibles suplantaciones de identidad o ataques de intermediario. El dispositivo configurador puede estar configurado para obtener la clave pública de cliente desde el dispositivo cliente, de tal manera que ninguna otra clave pública pueda usarse de forma indebida como la clave pública para el dispositivo cliente.

[14] Una red puede mantener una lista de dispositivos, y claves públicas asociadas, para coordinar el registro de un dispositivo en varios dispositivos de red. Por ejemplo, un dispositivo cliente agregado en un primer dispositivo de red puede registrarse en un segundo dispositivo de red en respuesta a que el primer dispositivo de red comparta la clave pública del dispositivo cliente con el segundo dispositivo de red. Además, cuando se elimina un dispositivo cliente de una red, la eliminación de la clave pública del dispositivo de la lista de dispositivos puede difundir la eliminación del dispositivo cliente entre otros dispositivos de red. Uno o más dispositivos de red de una red pueden mantener una lista de dispositivos cliente y una lista de dispositivos configuradores que están asociados con la red. Las claves públicas del (de los) dispositivo(s) cliente y el(los) dispositivo(s) configurador(es) pueden compartirse entre dispositivos fiables en la red.

[15] En algunos modos de realización, un dispositivo configurador puede certificar la clave pública de cliente para crear un certificado de cliente, y también puede certificar una clave pública de red para crear un certificado de red. El certificado de cliente y el certificado de red se pueden certificar usando una clave privada de configurador. Los certificados se podrían usar para facilitar el registro entre el dispositivo cliente y el dispositivo de red, ya que cada uno de estos dos dispositivos puede verificar la autenticidad de la clave pública de cliente y la clave pública de red.

[16] En la descripción anterior, el dispositivo configurador se puede usar en varios modos de realización diferentes. Por ejemplo, el dispositivo configurador puede usarse para transferir una única clave pública (por ejemplo, la clave pública de cliente del dispositivo cliente) al dispositivo de red. En otro ejemplo, el dispositivo configurador puede usarse para transferir dos claves públicas (por ejemplo, la clave pública de cliente y la clave pública de red) al dispositivo de red y al dispositivo cliente, respectivamente. En otro ejemplo, el dispositivo configurador también puede proporcionar una función de certificación a cada uno del dispositivo cliente y el dispositivo de red. En los diversos ejemplos, el dispositivo configurador puede utilizar una relación de confianza con el dispositivo de red y una comunicación fuera de banda con el dispositivo cliente para proporcionar confianza en que las claves públicas se comparten entre el dispositivo cliente correcto y el dispositivo de red correcto.

[17] La **figura 1** representa un sistema de ejemplo 100 en el que se puede usar la presente divulgación. En el sistema de ejemplo 100, un dispositivo cliente 110 puede estar dentro del alcance de comunicación de un dispositivo de red 120. El dispositivo cliente 110 puede ser un ordenador portátil, un teléfono inteligente, un aparato eléctrico o cualquier otro dispositivo que aún no haya sido autorizado por el dispositivo de red 120. El dispositivo de red 120 también puede denominarse dispositivo registrador. A modo de ejemplo, el dispositivo de red 120 puede ser un punto de acceso WLAN. Puede considerarse que el dispositivo cliente 110 está conectado de forma comunicativa con el dispositivo de red 120 después de aprovisionarse con el dispositivo de red 120. En algunos modos de realización, el dispositivo cliente 110 puede denominarse dispositivo registrado hasta que se ha aprovisionado apropiadamente mediante el dispositivo de red 120.

[18] En un escenario hipotético, un amigo o miembro de la familia (es decir, que es un usuario de un dispositivo cliente) que está de visita en una casa puede desear obtener acceso a una WLAN a través del punto de acceso. De forma alternativa, se puede proporcionar acceso a una WLAN para los huéspedes de un hotel, los invitados en un centro de convenciones o en un espacio público, pero se limita basándose en la autenticación. En implementaciones WLAN tradicionales, se puede requerir que un usuario del dispositivo cliente 110 introduzca un código de acceso u otra información para permitir que el dispositivo cliente 110 se autentique apropiadamente con el dispositivo de red 120. De acuerdo con la presente divulgación, el dispositivo cliente 110 puede aprovisionarse, en algunos modos de realización, sin que se requiera que el usuario introduzca manualmente un código de acceso o una clave de red. Además, la seguridad de la WLAN se puede mantener de tal forma que solo se permita el acceso a la WLAN a usuarios autorizados.

[19] Como se muestra en la figura 1, un dispositivo configurador 130 puede asistir en el aprovisionamiento del dispositivo cliente 110. El dispositivo configurador 130 puede ser un dispositivo informático (tal como un ordenador portátil, un ordenador personal, una tableta, un teléfono inteligente, un aparato eléctrico conectado en red o similar). En el ejemplo hipotético, el dispositivo configurador 130 es un dispositivo móvil que tiene una cámara, un procesador y una interfaz de red. El dispositivo configurador 130 está conectado de forma comunicativa al dispositivo de red 120. Para hacer que el dispositivo cliente 110 se registre en el dispositivo de red 120, el dispositivo configurador 130 puede obtener una clave pública de cliente asociada con el dispositivo cliente 110 y proporcionársela al dispositivo de red 120.

[20] En la presente divulgación, cuando se hace referencia a claves públicas y claves privadas, cada clave pública y clave privada pueden estar relacionadas como un par. Las claves privadas y públicas de un par pueden formar dos claves que están relacionadas matemáticamente pero son diferentes entre sí. La clave pública se puede usar para encriptar información o verificar una firma digital. La clave privada se puede usar para desencriptar la información o para crear una firma digital. Un experto en la materia puede designar este concepto mediante otros nombres, tales como criptografía de claves públicas o criptografía asimétrica. Debe entenderse que se pueden usar otros mecanismos de seguridad de forma adicional o alternativa a la encriptación de claves públicas. Por ejemplo, se pueden usar claves dinámicas, rotación de claves, algoritmos de troceo (*hash*) u otros mecanismos de forma adicional o alternativa a los mecanismos de claves públicas y de claves privadas descritos en el presente documento. Para simplificar, la criptografía de claves públicas se describe en la presente divulgación como un modo de realización de ejemplo.

[21] Como se muestra en la figura 1, la clave pública de cliente 154 puede obtenerse tomando una foto de una imagen con codificación de respuesta rápida (QR) 160 que tiene la clave pública de cliente 154 codificada en la misma. El dispositivo configurador 130 decodifica la clave pública de cliente 154 y proporciona la clave pública de cliente 154 al dispositivo de red 120 en un mensaje de registro 156. El dispositivo de red 120 puede usar la clave pública de cliente 154 en un proceso de registro y/o autenticación adicional (mostrado en 158), de tal manera que el dispositivo cliente 110 se agrega de manera comunicativa a la red sin pasar datos confidenciales sobre la red.

[22] El dispositivo configurador 130 puede extender las capacidades de registro del dispositivo de red 120 a un dispositivo móvil. Por ejemplo, el dispositivo de red 120 puede no estar equipado con capacidades de cámara, escáner, interfaz de radio de corto alcance o lector de etiquetas de comunicaciones de campo cercano (NFC). Además, el dispositivo de red 120 puede estar montado en una posición fija o en una ubicación de difícil acceso. Sin embargo, el dispositivo configurador 130 puede ser un dispositivo móvil y ser más adecuado para obtener la clave pública de cliente de un dispositivo cliente 110 que se agrega a la red. El dispositivo configurador 130 puede proporcionar la clave pública de cliente al dispositivo de red 120 para su uso en el registro del dispositivo cliente 110.

[23] Haciendo referencia al ejemplo del escenario doméstico anterior, un miembro de la familia o amigo pueden simplemente iniciar una aplicación que presenta (por ejemplo, visualiza una imagen codificada) la clave pública de cliente de su dispositivo cliente. El propietario de la vivienda puede agregar el dispositivo cliente a la red detectando la clave pública de cliente utilizando un dispositivo móvil que actúa como un dispositivo configurador 130. Del mismo modo, a los huéspedes de un hotel o invitados a una convención se les puede conceder acceso a servicios de red inalámbrica utilizando registro asistido sin necesidad de códigos de acceso ni configuraciones manuales complicadas.

[24] Debe entenderse que un dispositivo puede funcionar como el dispositivo configurador 130 en un entorno, mientras que funciona como el dispositivo cliente 110 en otro entorno. A modo de ejemplo, un dispositivo móvil que pertenece a la persona A se puede usar en la vivienda de la persona A como un dispositivo configurador 130 para un dispositivo de red 120 en la vivienda de la persona A. El mismo dispositivo móvil perteneciente a la persona A se puede usar como un dispositivo cliente 110 cuando el dispositivo móvil está en la vivienda de la persona B y para un dispositivo de red diferente (no mostrado) en la vivienda de la persona B. Por último, el dispositivo móvil también puede funcionar como el dispositivo de red 120, tal como cuando un dispositivo móvil se usa como un punto de concentración o como un propietario de grupo de igual a igual (P2P). En algunos modos de realización, las funciones del dispositivo de red 120 y el dispositivo configurador 130 pueden estar coubicadas o realizadas en el mismo aparato físico. Por ejemplo, el dispositivo móvil puede proporcionar un punto de concentración móvil a otros

dispositivos. Al mismo tiempo, el dispositivo móvil puede funcionar como un dispositivo configurador 130 para asistir en el registro de nuevos dispositivos cliente.

[25] Los escenarios hipotéticos anteriores se proporcionan con fines ilustrativos. Cabe señalar que pueden contemplarse muchos usos alternativos de la presente divulgación. En las descripciones anteriores, se describen varios modos de realización que pueden utilizar un dispositivo configurador para asistir en el aprovisionamiento de un nuevo dispositivo cliente.

[26] La **figura 2** representa un sistema de ejemplo 200 con detalles adicionales. De forma similar a la figura 1, un dispositivo cliente 110 puede estar dentro del alcance de comunicación de un dispositivo de red 120. En este ejemplo, un dispositivo configurador 130 puede asistir al dispositivo de red 120 en el aprovisionamiento del dispositivo cliente 110.

[27] El dispositivo configurador 130 puede establecer una relación de confianza 225 entre el dispositivo configurador 130 y el dispositivo de red 120. Ejemplos de la relación de confianza 225 se describen en mayor detalle con referencia a la figura 7. La relación de confianza 225 puede incluir el uso de claves de seguridad para autenticar y/o encriptar comunicaciones entre el dispositivo configurador 130 y el dispositivo de red 120. Además, la relación de confianza 225 representa una relación en la que el dispositivo configurador 130 está autorizado para asistir en el aprovisionamiento de nuevos dispositivos, tales como el dispositivo cliente 110.

[28] El establecimiento de la relación de confianza puede incluir etapas para que el dispositivo configurador 130 establezca una clave de relación de confianza para la relación de confianza 225. Por ejemplo, el dispositivo configurador 130 puede determinar una clave pública de red asociada con el dispositivo de red 120. El dispositivo configurador 130 puede tener una clave pública de configurador y una clave privada de configurador correspondiente. El dispositivo configurador 130 puede determinar la clave de relación de confianza basándose al menos en parte en la clave pública de red y la clave privada de configurador. De manera similar, el dispositivo de red 120 puede determinar la clave de relación de confianza basándose al menos en parte en la clave privada de red y la clave pública de configurador.

[29] En la figura 2, el dispositivo configurador 130 obtiene una clave pública de cliente (mostrada como una línea 254) asociada con el dispositivo cliente 110. El dispositivo cliente 110 puede tener una clave pública de cliente 254 y una clave privada de cliente correspondiente. El dispositivo configurador 130 puede obtener la clave pública de cliente 254, por ejemplo, usando un canal de comunicación o detección fuera de banda. Por ejemplo, el dispositivo configurador 130 puede utilizar una cámara para escanear una imagen asociada con el dispositivo cliente 110. La imagen puede ser una imagen 2D o 3D. Por ejemplo, la imagen puede ser un código de respuesta rápida (QR) o un código de barras. La imagen puede estar fijada al dispositivo cliente 110 o al embalaje asociado con el dispositivo cliente 110. El dispositivo configurador 130 puede usar otros tipos de canales de comunicación fuera de banda visuales, de audio o eléctricos para obtener la clave pública de cliente 254. Para simplificar, los ejemplos del presente documento se describen en términos de una imagen que tiene la clave pública de cliente codificada en la misma.

[30] En algunos modos de realización, la imagen puede ser estática o efímera. Por ejemplo, el dispositivo cliente 110 puede estar equipado con una pantalla y puede crear una imagen diferente para diferentes instancias de registro o para diferentes redes. La clave pública de cliente 254 puede determinarse escaneando y decodificando la imagen legible por máquina (por ejemplo, el código QR) con una cámara, un teléfono inteligente, un escáner u otro lector de códigos legibles por máquina del dispositivo configurador 130. El uso de una imagen legible por máquina, tal como un código QR, puede ayudar a determinar la clave pública de cliente de forma relativamente rápida, y puede reducir errores humanos asociados con la obtención o lectura de la clave pública de cliente. En otro modo de realización adicional, el fabricante puede proporcionar una etiqueta de comunicación de campo cercano (NFC, no mostrada) que contiene la clave pública de cliente 254, y fijarla al, o colocarla cerca del, dispositivo cliente 110. La etiqueta NFC puede leerse mediante un lector de etiquetas NFC para determinar la clave pública de cliente 254. El uso de la etiqueta NFC también puede reducir errores en la determinación de la clave pública de cliente 254 del dispositivo cliente 110.

[31] Una vez que el dispositivo configurador 130 ha obtenido la clave pública de cliente 254, el dispositivo configurador 130 puede enviar la clave pública de cliente 254 en un mensaje de registro 256 al dispositivo de red 120. En un modo de realización, antes de enviar el mensaje de registro 256, el dispositivo configurador 130 puede iniciar un registro enviando un mensaje de petición al dispositivo de red 120. El mensaje de petición (no mostrado) puede hacer que el dispositivo de red 120 proporcione un número arbitrario único (*nonce*) para el registro. El *nonce* puede ser un número aleatorio o pseudoaleatorio que puede proporcionar el dispositivo de red 120. El dispositivo configurador 130 puede usar el *nonce* para preparar una firma que acompañe a la clave pública de cliente 254. La firma también puede basarse en un proceso de encriptación y/o firma que demuestra que el dispositivo configurador 130 está autorizado para enviar el mensaje de registro 256. El mensaje de registro 256 puede incluir la clave pública de cliente 254 y la firma, así como otra información. Por ejemplo, el mensaje de registro 256 puede incluir información respecto a cómo se obtuvo la clave pública de cliente 254, una marca de tiempo, un identificador del dispositivo de red 120, un identificador de petición de registro y/u otra información. En un modo de realización, la

firma, el *nonce* o ambos pueden encriptarse mediante la clave de relación de confianza.

[32] Cuando el dispositivo de red 120 recibe el mensaje de registro 256, el dispositivo de red 120 puede verificar que la firma proviene de un dispositivo configurador 130 debidamente autorizado que tiene una relación de confianza 225 con el dispositivo de red 120. Si se verifica la firma, el dispositivo de red 120 puede usar la clave pública de cliente 254 del mensaje de registro 256 para completar el registro directamente con el dispositivo cliente 110. Por ejemplo, en un modo de realización, el dispositivo de red 120 puede iniciar el registro transmitiendo un mensaje de respuesta de sondeo (no mostrado) en respuesta a un mensaje de petición de sondeo. El mensaje de respuesta de sondeo puede incluir un *hash* u otra derivada de la clave pública de cliente. En otro modo de realización, el dispositivo de red 120 puede iniciar el registro y realizar una asociación inalámbrica inicial para establecer una sesión de comunicación con el dispositivo cliente 110, sobre la cual se puede intercambiar una autenticación y configuración adicionales.

[33] El registro y la autenticación del dispositivo cliente 110 pueden incluir un procedimiento de autenticación entre el dispositivo de red 120 y el dispositivo cliente 110. Por ejemplo, el dispositivo de red 120 puede enviar un mensaje de petición de autenticación 258 al dispositivo cliente 110. El mensaje de petición de autenticación 258 puede incluir la clave pública de red así como un *nonce* proporcionado por el dispositivo de red ("*nonce* proporcionado por la red"). El dispositivo cliente 110 puede generar un segundo *nonce* (o "*nonce* proporcionado por el cliente") y a continuación generar una clave compartida usando el *nonce* proporcionado por la red, el *nonce* proporcionado por el cliente, la clave pública de red y la clave privada de cliente. A continuación, el dispositivo cliente 110 puede enviar un mensaje de respuesta de autenticación 260 de vuelta al dispositivo de red 120. El mensaje 260 de respuesta de autenticación puede incluir el *nonce* proporcionado por el cliente y un código de autenticación de mensaje (MAC) del *nonce* proporcionado por el cliente. El MAC del *nonce* proporcionado por el cliente puede ser una función *hash* criptográfica del *nonce* proporcionado por el cliente (por ejemplo, que se ha preparado utilizando la clave compartida).

[34] El dispositivo de red 120 puede preparar de manera similar una clave compartida. La clave compartida se puede generar a partir del *nonce* proporcionado por la red, el *nonce* proporcionado por el cliente, la clave pública de cliente y la clave privada de red. El dispositivo de red 120 puede verificar que tiene la misma clave compartida que la generada por el dispositivo cliente 110 si el dispositivo de red 120 genera, a partir del *nonce* proporcionado por cliente y la clave compartida, un MAC igual al MAC incluido en el mensaje de respuesta de autenticación 260.

[35] Una vez que se ha verificado la existencia de la clave compartida, el dispositivo de red 120 puede considerar que el dispositivo cliente 110 está registrado. El dispositivo de red 120 puede usar la clave compartida para comunicaciones adicionales (no mostradas en la figura 2) entre el dispositivo de red 120 y el dispositivo cliente 110, tales como configuración, asociación de red o autenticación adicional. Por ejemplo, el dispositivo de red 120 puede enviar datos de configuración al dispositivo cliente 110. Los datos de configuración pueden incluir ajustes para el acceso inalámbrico, tales como un SSID del punto de acceso inalámbrico, canal o ajustes de potencia. Los datos de configuración también pueden incluir información adicional para seguridad, una capa de aplicación u otros ajustes usados por el dispositivo cliente 110 para comunicarse a través del dispositivo de red 120.

[36] Después del registro, en un modo de realización, el dispositivo cliente 110 y el dispositivo de red 120 pueden realizar una autenticación adicional (no mostrada en la figura 2). Por ejemplo, se puede llevar a cabo un procedimiento de negociación en 4 pasos entre el dispositivo cliente 110 y el dispositivo de red 120 para completar la autenticación y/o asociación del dispositivo cliente 110. Se puede usar una clave maestra en pares (PMK) para los subsiguientes mensajes de negociación y configuración de acceso Wi-Fi™ protegido (WPA). En un modo de realización, la clave compartida (SK) generada basándose en el *nonce* proporcionado por la red, el *nonce* proporcionado por el cliente, la clave pública de red y la clave privada de cliente se puede usar como PMK. De forma alternativa, la PMK puede obtenerse a partir de una SK. El dispositivo cliente puede obtener la PMK usando una función o algoritmo predeterminados que tienen al menos la SK como una variable de entrada. De forma similar, el dispositivo de red puede obtener la PMK usando la función o el algoritmo predeterminado y la misma SK. Por ejemplo, la PMK puede ser un *hash* de la SK. La PMK se puede usar a continuación para la negociación en 4 pasos u otras etapas de asociación/configuración entre el dispositivo cliente y el dispositivo de red.

[37] La **figura 3** representa un flujo de ejemplo 300 de operaciones que un dispositivo configurador (tal como el dispositivo configurador 130) puede realizar de acuerdo con algunos modos de realización. En el bloque 302, el dispositivo configurador puede establecer una relación de confianza con un dispositivo de red de una red. Ejemplos de establecimiento de una relación de confianza se proporcionan en las figuras 2 y 7.

[38] En el bloque 304, el dispositivo configurador puede determinar una clave pública de cliente asociada con un dispositivo cliente. Por ejemplo, determinar la clave pública de cliente puede incluir usar una cámara, un micrófono, un detector de luz, un escáner, una interfaz de radiofrecuencia de corto alcance (tal como Bluetooth™ o NFC) u otro sensor del dispositivo configurador para detectar la clave pública de cliente utilizando un medio fuera de banda. En algunos modos de realización, el procedimiento usado para determinar la clave pública de cliente puede requerir proximidad entre el dispositivo configurador y el dispositivo cliente, para proteger contra acceso remoto no deseado o violaciones de seguridad.

[39] En el bloque 308, el dispositivo configurador puede enviar la clave pública de cliente asociada con el dispositivo cliente de acuerdo con la relación de confianza, y la clave pública de cliente se usará para la autenticación entre el dispositivo de red y el dispositivo cliente.

[40] La **figura 4** es un diagrama de flujo de mensajes que ilustra un ejemplo de aprovisionamiento de dispositivos asistido utilizando un dispositivo configurador para proporcionar una clave pública de cliente a un dispositivo de red, de acuerdo con modos de realización de la presente divulgación. En el flujo de mensajes de ejemplo 400 de la figura 4, un dispositivo configurador 130 puede obtener la clave pública de cliente 414 utilizando un medio de comunicación fuera de banda unidireccional. El dispositivo configurador 130 ha establecido una relación de confianza 402 con el dispositivo de red 120. En algunos modos de realización, la relación de confianza 402 puede configurarse previamente antes del momento en que el dispositivo configurador obtiene la clave pública de cliente del dispositivo cliente 110. De forma alternativa, la relación de confianza 402 puede establecerse en respuesta a o después de que el dispositivo configurador obtiene la clave pública de cliente asociada con el dispositivo cliente 110.

[41] Después de establecer la relación de confianza 402, el dispositivo de red 120 puede almacenar información 404 con respecto al dispositivo configurador 130, tal como una clave pública de configurador, un identificador, un período de autorización o similar. La información almacenada 404 puede usarse posteriormente, tal como para verificar la autorización del dispositivo configurador 130 y/o asistir en el registro y la autenticación del dispositivo cliente 110. Por ejemplo, la información almacenada 404 se puede usar para desencriptar o verificar una firma proporcionada por el dispositivo configurador 130 en un mensaje de registro.

[42] El dispositivo configurador 130 puede usar un medio fuera de banda para obtener la clave pública de cliente 414 del dispositivo cliente 110. Por ejemplo, la clave pública de cliente se puede obtener a través de una cámara y una imagen, señales de radiofrecuencia de corto alcance (como Bluetooth o NFC) u otro medio fuera de banda. En algunos modos de realización, el dispositivo configurador 130 puede consultar 412 opcionalmente al dispositivo cliente 110 para obtener la clave pública de cliente 414. En algunos modos de realización, el dispositivo configurador 130 puede no consultar 412 al dispositivo cliente 110, tal como cuando la clave pública de cliente 414 se obtiene escaneando una imagen codificada. La clave pública de cliente puede ser estática o efímera. Si la clave pública de cliente es efímera, el dispositivo cliente 110 puede generar una clave pública de cliente y proporcionar la clave pública de cliente al dispositivo configurador 130 en respuesta a la consulta 412. En otros casos, la clave pública de cliente puede ser estática. Si el medio fuera de banda no admite comunicación bidireccional, el dispositivo configurador 130 puede simplemente detectar la clave pública de cliente utilizando un sensor, un micrófono, un detector de luz, una cámara u otras capacidades del dispositivo configurador.

[43] El dispositivo configurador 130 puede iniciar una sesión de registro enviando una petición de registro 420 al dispositivo de red 120. El dispositivo de red 120 puede enviar una respuesta 422 con un *nonce* (que también puede denominarse *nonce* de registro o identificador de sesión de registro). El *nonce* puede ser un número aleatorio o pseudoaleatorio proporcionado por el dispositivo de red 120. En algunas implementaciones, el *nonce* puede generarse mediante el dispositivo configurador 130 y proporcionarse en la petición de registro 420, y confirmarse mediante la respuesta 422. El uso de un *nonce* puede prevenir los denominados ataques de reproducción que son una violación de seguridad en la que se usa un intercambio de mensajes previamente usados para introducir datos no autorizados.

[44] El dispositivo configurador 130 puede proporcionar la clave pública de cliente del dispositivo cliente 110 al dispositivo de red 120 en un mensaje de registro 424. Como se ha descrito previamente, el mensaje de registro 424 puede incluir otra información, tal como una firma que se obtiene a partir del *nonce* de registro. La firma puede usarse para verificar (mostrado en el procedimiento de verificación 426) la autoridad del dispositivo configurador 130 antes de proceder con el registro del dispositivo cliente 110. Si se verifica, la clave pública de cliente puede almacenarse para su uso en un proceso de autenticación.

[45] En respuesta al mensaje de registro 424 y la verificación de la firma, el dispositivo de red 120 puede realizar un procedimiento de registro 430. El procedimiento de registro puede incluir uno o más de un mensaje de baliza, un mensaje de petición de sondeo, un mensaje de respuesta de sondeo, un mensaje de comienzo de autenticación, un mensaje de iniciación de autenticación, una petición de asociación y una respuesta de asociación. Estos mensajes pueden denominarse etapas de detección que se usan para establecer una comunicación inicial entre el dispositivo cliente 110 y el dispositivo de red 120, sobre los que puede producirse una autenticación y configuración adicionales. En un ejemplo, el procedimiento de registro 430 incluye el establecimiento de un canal de autenticación que puede usarse mediante un protocolo de autenticación, tal como un protocolo de autenticación extensible (EAP).

[46] Un proceso de autenticación de ejemplo puede incluir un mensaje de petición de autenticación 432 (similar al mensaje de petición de autenticación 258) y un mensaje de respuesta de autenticación 434 (similar al mensaje de respuesta de autenticación 260). Como se describe en la figura 2, el proceso de autenticación puede incluir el uso de un *nonce* proporcionado por la red (en un mensaje de petición de autenticación 432) y un *nonce* proporcionado por el cliente (en un mensaje de respuesta de autenticación 434) para determinar una clave compartida entre el dispositivo cliente 110 y el dispositivo de red 120.

[47] Después del mensaje de petición de autenticación 432 y el mensaje de respuesta de autenticación 434, puede tener lugar un proceso de configuración. Por ejemplo, el dispositivo de red 120 puede transmitir datos de configuración 436 al dispositivo cliente 110. Los datos de configuración 436 pueden incluir información tal como un SSID del punto de acceso, información del canal inalámbrico (tal como un identificador de canal), claves de capa de aplicación, etc. En un ejemplo, los datos de configuración 436 pueden protegerse basándose al menos en parte en la clave compartida. Por ejemplo, los datos de configuración 436 pueden encriptarse utilizando la clave compartida o una derivada de la clave compartida.

[48] La clave compartida también se puede usar en un subsiguiente proceso de autenticación usado para el acceso a la red. Por ejemplo, una autenticación adicional (no mostrada en la figura 1) puede incluir un procedimiento de negociación en 4 pasos realizado entre el dispositivo cliente 110 y el dispositivo de red 120. El procedimiento de negociación en 4 pasos puede basarse en una clave maestra en pares que se obtiene a partir de la clave compartida.

[49] El dispositivo de red 120 puede enviar un mensaje de confirmación 440 al dispositivo configurador 130 para confirmar que el dispositivo cliente 110 se ha registrado y/o autenticado con éxito en la red. En respuesta al mensaje de confirmación 440, el dispositivo configurador 130 puede proporcionar una señal visual, auditiva y/o de otro tipo para indicar al usuario que el registro y/o autenticación de red se ha completado con éxito.

[50] La **figura 5** es un diagrama de flujo de mensajes que ilustra un ejemplo de aprovisionamiento de dispositivos asistido en el que un dispositivo cliente supervisa un canal predeterminado, de acuerdo con modos de realización de la presente divulgación. En el flujo de mensajes de ejemplo 500 de la figura 5, un dispositivo configurador 130 o dispositivo de red 120 aprovisiona un dispositivo cliente 110 sobre un canal predeterminado temporal. El dispositivo configurador 130 ha establecido una relación de confianza 402 con el dispositivo de red 120. Después de establecer la relación de confianza 402, el dispositivo configurador 130 puede usar un medio fuera de banda para obtener (mostrado en 414) la clave pública de cliente del dispositivo cliente 110. Por ejemplo, el dispositivo configurador 130 puede escanear un código QR asociado con el dispositivo cliente 110. El dispositivo configurador 130 puede enviar un mensaje de registro 424 que tiene la clave pública de cliente al dispositivo de red 120. En este ejemplo, el dispositivo cliente 110 se aprovisiona usando un canal predeterminado. Por ejemplo, el dispositivo cliente 110 puede supervisar 521 un canal predeterminado para detectar un mensaje de baliza que inicia el aprovisionamiento de dispositivos. En un modo de realización, el dispositivo cliente 110 puede supervisar el canal predeterminado si todavía no tiene una conexión de red. De forma alternativa, el dispositivo cliente 110 puede supervisar periódicamente el canal predeterminado para detectar un mensaje de baliza procedente de cualquier dispositivo de red que desea aprovisionar el dispositivo cliente 110.

[51] El dispositivo de red 120 o bien el dispositivo configurador 130 puede acceder temporalmente al canal predeterminado para enviar un mensaje de baliza. Por ejemplo, el dispositivo de red 120 puede enviar un mensaje de baliza 526 sobre el canal predeterminado. En otro ejemplo, el dispositivo configurador 130 puede enviar un mensaje de baliza 528 sobre el canal predeterminado. Se podrían usar otros tipos de mensajes de detección, además o en lugar de un mensaje de baliza. El aprovisionamiento de dispositivos (por ejemplo, registro y/o autenticación) puede continuar tal como se ha descrito previamente (ver las descripciones correspondientes de los mensajes 430-440 en la figura 4).

[52] La **figura 6** es un diagrama de flujo de mensajes que ilustra un ejemplo de aprovisionamiento de dispositivos asistido en el que un dispositivo configurador proporciona una clave de registro a un dispositivo cliente, de acuerdo con modos de realización de la presente divulgación. En el flujo de mensajes 600 de ejemplo de la figura 6, el dispositivo configurador 130 puede obtener la clave pública de cliente 614 utilizando un medio de comunicación fuera de banda bidireccional. En este ejemplo, el dispositivo configurador 130 también puede proporcionar una clave pública de red 630 (que también puede denominarse clave pública de registro).

[53] El dispositivo configurador 130 ha establecido una relación de confianza 602 con el dispositivo de red 120. Después de establecer la relación de confianza 602, el dispositivo de red 120 puede almacenar información 604 con respecto al dispositivo configurador 130, tal como una clave pública de configurador, un identificador, un período de autorización o similar.

[54] El dispositivo configurador 130 puede usar una interfaz fuera de banda 606 para obtener la clave pública de cliente del dispositivo cliente 110 a través de un medio fuera de banda y una interfaz fuera de banda 605. En el ejemplo de la figura 6, el medio fuera de banda admite comunicación bidireccional. El medio fuera de banda es diferente del medio de comunicación cuyo acceso controla el dispositivo de red 120. Por lo tanto, el dispositivo cliente 110 y el dispositivo configurador 130 pueden configurarse con una interfaz de comunicación alternativa, tal como una interfaz de radiofrecuencia de corto alcance, redes inalámbricas de igual a igual, un medio cableado directamente u otro medio de comunicaciones que admita comunicación bidireccional. El dispositivo configurador 130 puede enviar un mensaje de consulta 612 al dispositivo cliente 110 para obtener la clave pública de cliente del dispositivo cliente 110. En respuesta al mensaje de consulta 612, el dispositivo cliente 110 puede responder con un mensaje de respuesta 614 que incluye la clave pública de cliente.

[55] De forma similar a los mensajes 420-424 de la figura 4, el dispositivo configurador 130 puede enviar una petición de registro 620 al dispositivo de red 120, recibir una respuesta 622 con un *nonce* (que también puede denominarse *nonce* de registro o identificador de sesión de registro), y enviar un mensaje de registro 624 que tiene la clave pública de cliente y una firma basada al menos en parte en el *nonce* de registro. La firma puede usarse en el procedimiento de verificación 625 para verificar la autoridad del dispositivo configurador 130 antes de proceder con el registro del dispositivo cliente 110. Si se verifica, la clave pública de cliente puede almacenarse para su uso en un proceso de autenticación.

[56] En el ejemplo de la figura 6, el dispositivo de red 120 puede proporcionar una clave de registro 626 al dispositivo configurador 130. La clave de registro 626 también se puede denominar clave pública de red asociada con el dispositivo de red 120. Sin embargo, en el ejemplo de la figura 6, la clave de registro 626 es una clave de registro de uso único proporcionada para que el dispositivo configurador 130 la envíe al dispositivo cliente 110 utilizando el medio de comunicaciones de dos vías bidireccional. El dispositivo configurador 130 proporciona la clave de registro 630 al dispositivo cliente 110. La clave de registro puede ser una clave pública que tiene una clave privada correspondiente almacenada en el dispositivo de red 120. En algunos ejemplos, el dispositivo configurador 130 puede enviar una clave pública de red o una clave de registro que el dispositivo configurador 130 conoce previamente. Por ejemplo, el dispositivo de red 120 puede proporcionar una clave de registro al dispositivo configurador 130 después de establecer la relación de confianza 602. La clave de registro puede tener un tiempo de validez y/o puede ser exclusiva para el dispositivo configurador particular 130. De forma alternativa, si se proporciona en el mensaje 626, la clave de registro podría ser específica para el dispositivo cliente 110.

[57] En 631, el dispositivo de red 120 puede realizar etapas de detección para establecer una comunicación inicial entre el dispositivo cliente 110 y el dispositivo de red 120. Las etapas de detección se pueden modificar para usar la clave de registro. Por ejemplo, la clave de registro (o una derivada de la misma) puede usarse en un mensaje de petición de sondeo o un mensaje de respuesta de sondeo como una forma para verificar la identidad del dispositivo cliente 110 y/o el dispositivo de red 120. De forma alternativa, la clave de registro (o una derivada de la misma) puede incluirse en un mensaje de baliza del dispositivo de red 120. Si no se puede verificar la identidad del dispositivo cliente 110 o el dispositivo de red 120, entonces el proceso de registro puede terminar, evitando que cualquier comunicación o autenticación adicional innecesaria consuma recursos de procesador o red.

[58] De forma similar a las figuras 2 y 4, el proceso de autenticación de ejemplo puede incluir un mensaje de petición de autenticación 632 y un mensaje de respuesta de autenticación 634. A diferencia de la figura 4, en la figura 6, el mensaje de petición de autenticación 632 puede no incluir una clave pública de red, ya que el dispositivo configurador 130 ya ha proporcionado la clave de registro al dispositivo cliente 110 utilizando el medio de comunicaciones fuera de banda bidireccional. En cambio, el mensaje de petición de autenticación 632 puede incluir el *nonce* proporcionado por la red, pero puede no incluir la clave pública de red. A continuación, como se describe en las figuras 2 y 4, el proceso de autenticación puede incluir el uso de un *nonce* proporcionado por la red (en un mensaje de petición de autenticación 632), un *nonce* proporcionado por el cliente (en un mensaje de respuesta de autenticación 634) y sus respectivas claves privadas y la clave pública del otro para determinar una clave compartida entre el dispositivo cliente 110 y el dispositivo de red 120. En 636, un proceso de configuración puede incluir la transmisión de datos de configuración desde el dispositivo de red 120 al dispositivo cliente 110.

[59] El dispositivo de red 120 puede enviar un mensaje de confirmación 640 al dispositivo configurador 130 para confirmar que el dispositivo cliente 110 se ha registrado y autenticado correctamente en la red. En respuesta al mensaje de confirmación 640, el dispositivo configurador 130 puede proporcionar una señal visual, auditiva y/o de otro tipo para indicar al usuario que el registro y la autenticación de la red se han completado con éxito.

[60] La **figura 7** representa un flujo de mensajes de ejemplo 700 para establecer una relación de confianza entre el dispositivo configurador 130 y el dispositivo de red 120. El dispositivo de red 120 puede transmitir un mensaje de anuncio de servicio de compatibilidad con configurador 702. El mensaje de anuncio de servicio de compatibilidad con configurador puede ser parte de un mensaje de baliza o un mensaje de tara. Por ejemplo, el mensaje de anuncio de servicio de compatibilidad con configurador puede estar incluido en un mensaje que indica las capacidades del dispositivo de red 120. El mensaje de anuncio de servicio de compatibilidad con configurador 702 puede indicar al dispositivo configurador 130 que el dispositivo de red 120 admite el uso de registro y autenticación asistidos, tal como se describe en la presente divulgación.

[61] El dispositivo configurador 130 puede usar un medio fuera de banda para obtener una clave pública de red asociada con el dispositivo de red 120. Por ejemplo, el dispositivo configurador 130 puede enviar un mensaje de consulta 708 al dispositivo de red 120 para solicitar la clave pública de red. El dispositivo de red 120 puede proporcionar la clave pública de red en un mensaje de respuesta 709. De forma alternativa, el dispositivo configurador 130 puede simplemente usar una cámara, un escáner de código de barras, una interfaz de radiofrecuencia de corto alcance o un lector de etiquetas NFC para detectar la clave pública de red. En un ejemplo, el dispositivo configurador 130 obtiene la clave pública de red decodificando una imagen que tiene datos codificados por máquina. El dispositivo configurador 130 también puede obtener otra información, tal como un identificador (ID) o información de configuración del dispositivo de red. En un modo de realización, el identificador puede obtenerse a

partir de la clave pública de red. La información de configuración puede incluir información del canal predeterminado.

[62] El dispositivo configurador 130 y el dispositivo de red 120 pueden realizar etapas de detección 712, 714 para establecer una comunicación inicial entre el dispositivo configurador 130 y el dispositivo de red 120. Las etapas de detección 712, 714 pueden ser similares a las descritas en las figuras 4-6. Las etapas de detección también se pueden usar para verificar que el dispositivo configurador 130 y el dispositivo de red 120 deben continuar con el establecimiento de la relación de confianza. Por ejemplo, el dispositivo configurador 130 puede transmitir un mensaje de petición de sondeo que incluye el ID del dispositivo de red. El dispositivo de red 120 puede verificar que el ID coincide con el ID correcto del dispositivo de red, y después responder con un mensaje de respuesta de sondeo. Si no se puede verificar el ID del dispositivo de red 120, entonces el dispositivo de red 120 puede interrumpir la comunicación con el dispositivo configurador 130 y/o evitar que se establezca la relación de confianza.

[63] El dispositivo configurador 130 puede enviar un mensaje de petición de autenticación 716 al dispositivo de red 120 con una indicación de que el dispositivo configurador 130 desea autoridad para actuar como dispositivo configurador para el dispositivo de red 120. El mensaje de petición de autenticación 716 puede incluir la clave pública de configurador y un *nonce* proporcionado por el configurador. Además, el mensaje de petición de autenticación 716 puede indicar otra información, tal como el procedimiento usado para obtener la clave pública de red, un identificador del dispositivo configurador 130 u otra información.

[64] El dispositivo de red 120 puede usar el *nonce* proporcionado por el configurador, la clave pública de configurador, un *nonce* proporcionado por la red y una clave privada de red para determinar una clave de relación de confianza 625. El dispositivo de red 120 puede usar la clave compartida para encriptar el *nonce* proporcionado por la red. Opcionalmente, también puede encriptarse otra información con el *nonce* proporcionado por la red, tal como un identificador de conjunto de servicios (SSID) de una WLAN, u otra información de configuración de red. Por ejemplo, el dispositivo de red 120 puede generar un MAC basándose al menos en parte en el SSID y el *nonce* proporcionado por la red.

[65] En el mensaje de respuesta de autenticación 718, el dispositivo de red 120 proporciona el *nonce* proporcionado por la red y el MAC al dispositivo configurador 130. Si el SSID se ha usado para generar el MAC, el SSID se puede incluir opcionalmente en el mensaje de respuesta de autenticación 718.

[66] El dispositivo configurador 130 puede usar el *nonce* proporcionado por la red, el *nonce* proporcionado por el configurador, la clave privada de configurador y la clave pública de red para determinar la clave de relación de confianza 722. El dispositivo configurador 130 puede usar la clave de relación de confianza para calcular un MAC para verificar que el MAC generado por el configurador coincide con el MAC proporcionado por la red en el mensaje de respuesta de autenticación 718.

[67] El dispositivo de red 120 puede almacenar 732 la clave pública de configurador y, opcionalmente, la clave de relación de confianza para su uso posterior. Por ejemplo, la clave pública de configurador puede almacenarse en una lista de dispositivos configuradores autorizados. La clave pública de configurador puede almacenarse durante un tiempo limitado y puede eliminarse una vez transcurrido un período de tiempo. De forma alternativa, el dispositivo configurador puede enviar un mensaje (no mostrado) que indica que ya no está actuando como dispositivo configurador para la red. El dispositivo de red puede eliminar la clave pública de configurador y la clave de relación de confianza. El dispositivo de red puede configurarse para eliminar todas las claves públicas de configurador después de un reinicio o restablecimiento. Además, el dispositivo de red puede limitar la cantidad de dispositivos configuradores aprobados simultáneamente.

[68] En un modo de realización, la relación de confianza también se puede usar para intercambiar datos de configuración. Por ejemplo, pueden transmitirse uno o más mensajes de configuración 742, 744 para transportar datos de configuración. En un ejemplo, el dispositivo de red 120 puede transmitir los datos de configuración actuales 742 al dispositivo configurador 130. En otro ejemplo, el dispositivo configurador 130 puede transmitir nuevos datos de configuración 744 al dispositivo de red 120.

[69] En un modo de realización, se pueden realizar mensajes y procedimientos similares en un entorno de igual a igual entre dos dispositivos. En otras palabras, en un modo de realización, el dispositivo configurador 130 y el dispositivo de red 120 de la figura 7 pueden ser dispositivos iguales que establecen una relación de igual a igual utilizando mensajes similares a los que se usarían para establecer la relación de confianza descrita anteriormente. En el modo de realización de igual a igual, los dispositivos pueden realizar un procedimiento de detección de igual a igual y una negociación de grupo antes de intercambiar claves públicas. A menudo, en entornos de igual a igual uno de los dispositivos puede actuar como administrador de grupo, con funcionalidades similares a las del dispositivo de red 120 descrito.

[70] En otro modo de realización, se pueden realizar mensajes y procedimientos similares para un aprovisionamiento de dispositivos directamente entre un dispositivo cliente 110 y un dispositivo de red 120. En otras palabras, el dispositivo configurador 130 de la figura 7 puede comportarse como un dispositivo cliente que aún no está aprovisionado para la red asociada con el dispositivo de red 120. El dispositivo cliente puede establecer una

conexión de red utilizando mensajes similares a los que se usarían para establecer la relación de confianza descrita anteriormente.

[71] La **figura 8** representa otro ejemplo de aprovisionamiento de dispositivos en el que se ilustran un dispositivo cliente 110 y un dispositivo de red 120. El dispositivo cliente 110 puede obtener (en 709) la clave pública de red del dispositivo de red 120. En la figura 8, la clave pública de red se obtiene a través de un medio fuera de banda. Por ejemplo, el dispositivo cliente 110 puede escanear un código QR asociado con el dispositivo de red 120, en el que el código QR incluye la clave pública de red codificada en la imagen. El dispositivo de red 120 puede incluir la clave pública de red (o una derivada de esta) en un primer mensaje 811 del dispositivo de red 120. Por ejemplo, el primer mensaje 811 puede ser un mensaje de anuncio de servicio, una respuesta de sondeo, un mensaje de tara o un mensaje de baliza. En un modo de realización, se puede incluir una derivada (tal como un *hash*) de la clave pública de red en el primer mensaje 811. El dispositivo cliente 110 puede explorar pasivamente una pluralidad de canales hasta identificar un canal con el primer mensaje 811 que tiene la clave pública de red (o derivada). De esta forma, el dispositivo cliente 110 puede identificar el canal apropiado para continuar el proceso de aprovisionamiento. El proceso de aprovisionamiento (mostrado en 712-744) puede ser similar al proceso descrito en la figura 7.

[72] En otro modo de realización de la figura 8, el dispositivo cliente 110 puede usar una exploración activa en una pluralidad de canales para identificar un canal administrado por el dispositivo de red 120. El dispositivo cliente 110 puede enviar un mensaje de petición de sondeo 810 y recibir una respuesta de sondeo (como el primer mensaje 811). Si la respuesta de sondeo incluye la clave pública de red (o una derivada de la clave pública de red), el dispositivo cliente 110 puede identificar ese canal como el canal apropiado para continuar el aprovisionamiento de dispositivos.

[73] Como se ha descrito anteriormente, los mensajes descritos en las figuras 7-8 se podrían usar para varios escenarios, incluyendo el establecimiento de una relación de confianza para un dispositivo configurador, la creación de una red de igual a igual o la conexión de un nuevo dispositivo cliente a una red En la figura 7, después de un proceso de detección inicial, dos dispositivos intercambian claves públicas. Las claves públicas se usan con claves privadas en cada dispositivo para determinar una clave derivada usada para aprovisionar un dispositivo para el otro dispositivo. Como se observa en las figuras anteriores, se puede usar un tercer dispositivo (por ejemplo, un dispositivo configurador 130) como intermediario entre el primer y el segundo dispositivos (por ejemplo, el dispositivo cliente 110 y el dispositivo de red 120). Las siguientes figuras proporcionan ejemplos adicionales de un dispositivo intermediario que realiza funciones similares a las descritas anteriormente con respecto al dispositivo configurador 130.

[74] La **figura 9** representa un sistema de ejemplo 900 en el que la funcionalidad de un dispositivo configurador puede implementarse en un servicio configurador fiable 131 tal como un servicio basado en red (por ejemplo, "nube"). La figura 9 incluye un dispositivo cliente 110 y un dispositivo de red 120. Inicialmente, se considera que el dispositivo cliente 110 no está registrado en el dispositivo de red 120.

[75] Utilizando un medio de comunicación fuera de banda, el dispositivo cliente 110 puede proporcionar la clave pública de cliente (en un primer mensaje 914) al servicio configurador fiable 131. El servicio configurador fiable 131 puede proporcionar la clave pública de cliente (en un segundo mensaje 924) al dispositivo de red 120. De forma similar, el dispositivo de red 120 puede proporcionar la clave pública de red (en un tercer mensaje 916) al servicio configurador fiable 131. El servicio configurador fiable 131 puede proporcionar la clave pública de red (en un cuarto mensaje 926) al dispositivo cliente 110.

[76] El servicio configurador fiable 131 puede servir como un centro de intercambio de claves públicas o una autoridad de claves. En un modo de realización, el dispositivo cliente 110 y el dispositivo de red 120 pueden proporcionar la clave pública de cliente y la clave pública de red, respectivamente, antes de cualquier asociación potencial entre el dispositivo cliente 110 y el dispositivo de red 120. Por ejemplo, el servicio configurador fiable 131 puede ser un repositorio basado en la nube que almacena las claves públicas de múltiples dispositivos cliente y dispositivos de red, de tal manera que se puede establecer una relación entre un dispositivo cliente particular y un dispositivo de red particular simplemente administrando la distribución de las claves públicas

[77] En un modo de realización, el servicio configurador fiable 131 puede establecer una relación fiable con uno o ambos del dispositivo cliente 110 y el dispositivo de red 120. La clave pública de cliente y la clave pública de red se pueden proporcionar utilizando un enlace de comunicaciones seguro de acuerdo con la relación de confianza.

[78] El dispositivo cliente 110 o bien el dispositivo de red 120 puede iniciar el proceso de registro 931 basándose en la clave pública recibida del servicio configurador fiable 131. El proceso de registro 931 puede incluir las etapas de detección, como se describe en las figuras 4-8. Después de las etapas de detección, el dispositivo cliente 110 puede iniciar el proceso de autenticación enviando un mensaje de petición de autenticación 934 al dispositivo de red 120. El mensaje de petición de autenticación 934 puede incluir un *nonce* proporcionado por el cliente y, opcionalmente, puede incluir información adicional relativa al dispositivo cliente 110. El dispositivo de red 120 puede generar un *nonce* proporcionado por la red y usar el *nonce* proporcionado por la red, el *nonce*

proporcionado por el cliente, la clave privada de red y la clave pública de cliente (del servicio configurador fiable 131) para determinar la clave compartida. En el mensaje de respuesta de autenticación 932, el dispositivo de red 120 puede incluir el *nonce* proporcionado por la red, así como un MAC basado al menos en parte en la clave compartida.

[79] El dispositivo cliente 110 puede usar el *nonce* proporcionado por la red, el *nonce* proporcionado por el cliente, la clave privada de cliente y la clave pública de red para determinar la misma clave compartida. La clave compartida se verifica generando un MAC y comparando el MAC generado por el cliente con el MAC recibido.

[80] Después del registro y la autenticación, el dispositivo de red 120 puede proporcionar datos de configuración 952 al dispositivo cliente 110. Además, se puede realizar (no mostrada) una autenticación adicional (tal como una negociación en 4 pasos o un establecimiento de una PMK).

[81] La **figura 10** representa otro sistema de ejemplo 1000 en el que un servicio configurador 131 puede asistir en la autenticación entre un dispositivo cliente 110 y un dispositivo de red 120. En un ejemplo, el servicio configurador 131 puede ser un servicio fiable (por ejemplo, en la nube). En un modo de realización, el servicio configurador fiable 131 puede proporcionar una certificación fiable adicional de la clave pública de cliente y la clave pública de red. Una certificación incluye la "firma" o certificación de un paquete de información mediante encriptación del paquete de información utilizando una clave privada. Como resultado del proceso de certificación, se puede generar un "certificado".

[82] Utilizando un medio de comunicación fuera de banda, el dispositivo cliente 110 puede proporcionar la clave pública de cliente (en un primer mensaje 1014) al servicio configurador fiable 131. El servicio configurador fiable 131 puede firmar la clave pública de cliente usando una clave privada de configurador para generar un certificado de cliente. El certificado de cliente puede verificarse usando la clave pública de configurador, que el dispositivo cliente y el dispositivo de red pueden conocer.

[83] De forma similar, el dispositivo de red 120 puede proporcionar la clave pública de red (en un segundo mensaje 1016) al servicio configurador fiable 131. El servicio configurador fiable 131 también puede generar un certificado de red firmando la clave pública de red con la clave privada de configurador.

[84] El servicio configurador fiable 131 puede enviar la clave pública de configurador y el certificado de red en un tercer mensaje 1024 al dispositivo de red 120. La clave pública de configurador también puede denominarse clave pública de autoridad de certificación (CA). El servicio configurador fiable 131 puede enviar la clave pública de configurador y el certificado de cliente en un cuarto mensaje 1026 al dispositivo cliente 110. Por lo tanto, cada uno del dispositivo cliente y el dispositivo de red tendrá la clave pública de configurador, así como una copia certificada por el configurador de su propia clave pública. Cada uno del certificado de cliente y el certificado de red puede incluir una firma proporcionada por el servicio configurador fiable 131. La firma se puede calcular basándose en una parte del certificado y la clave privada de configurador. Por ejemplo, una parte de datos del certificado se puede usar para crear un compendio o *hash* del mensaje. El compendio o *hash* del mensaje se puede encriptar entonces utilizando una clave privada de configurador para generar la firma. La firma se puede agregar como una segunda parte del certificado.

[85] El dispositivo cliente 110 o bien el dispositivo de red 120 pueden iniciar el registro en respuesta a la recepción de la copia certificada por el configurador de su propia clave pública y la verificación de la autenticidad de la firma. El registro puede comenzar con etapas de detección 1031 para establecer un canal de comunicación inicial entre el dispositivo cliente 110 y el dispositivo de red 120 sobre el que se puede usar un protocolo de autenticación. El protocolo de autenticación puede incluir un mensaje de petición de autenticación 1034 y un mensaje de respuesta de autenticación 1032.

[86] El dispositivo cliente 110 puede incluir el certificado de cliente y un *nonce* proporcionado por el cliente en el mensaje de petición de autenticación 1034. Tras recibir el certificado de cliente, el dispositivo de red 120 puede verificar el certificado de cliente en el procedimiento de verificación 1046. Por ejemplo, el dispositivo de red 120 puede usar una clave pública de configurador para verificar el certificado de cliente. Para verificar que el certificado se emitió mediante el servicio configurador fiable 131, un dispositivo destinatario puede usar la clave pública de configurador para desencriptar la firma a fin de obtener el compendio o *hash* del mensaje de firma. El dispositivo destinatario puede calcular a continuación un compendio o *hash* del mensaje recibido a partir de la parte de datos y comparar el compendio/*hash* del mensaje recibido con el compendio/*hash* del mensaje de firma. El dispositivo de red 120 puede determinar la clave compartida. Por ejemplo, el dispositivo de red 120 puede generar un *nonce* proporcionado por la red y determinar la clave compartida usando el *nonce* proporcionado por el cliente, la clave pública de cliente extraída del certificado de cliente, la clave privada de red y el *nonce* proporcionado por la red.

[87] En el mensaje de respuesta de autenticación 1032, el dispositivo de red 120 puede incluir el *nonce* proporcionado por la red, el certificado de red y un MAC del *nonce* proporcionado por el cliente. El MAC del *nonce* proporcionado por el cliente puede ser una función *hash* criptográfica del *nonce* proporcionado por el cliente que se ha preparado usando la clave compartida.

[88] En el procedimiento de verificación 1042, el dispositivo cliente puede verificar el certificado de red utilizando la clave pública de configurador. Si está verificado, el dispositivo cliente 110 puede usar la clave pública de red almacenada en el certificado de red y generar la misma clave compartida mediante el *nonce* proporcionado por la red, el *nonce* proporcionado por el cliente, la clave pública de red y la clave pública de cliente, utilizando un proceso similar usado por el dispositivo de red 120.

[89] Una vez que se ha obtenido la clave compartida, el dispositivo cliente 110 y el dispositivo de red 120 pueden usar la clave compartida para una subsiguiente autenticación de negociación de 4 pasos y/o etapas de configuración 1052.

[90] La **figura 11** representa otro sistema de ejemplo 1100 en el que un dispositivo configurador puede realizarse como un punto de acceso 1130 para facilitar una conexión inalámbrica de igual a igual directa entre un primer dispositivo cliente 1110 y un segundo dispositivo cliente 1120. Inicialmente, el primer dispositivo cliente 1110 y el segundo dispositivo cliente 1120 pueden tener una asociación inalámbrica con un punto de acceso 1130, pero pueden no tener una asociación inalámbrica de igual a igual directa entre sí.

[91] El punto de acceso 1130 se puede configurar para proporcionar claves públicas al primer y segundo dispositivos cliente 1110, 1120. En un modo de realización, el punto de acceso 1130 puede obtener la primera clave pública de cliente (en un primer mensaje 1114) del primer dispositivo cliente 1110 y proporcionar la primera clave pública de cliente (en un segundo mensaje 1124) al segundo dispositivo cliente 1120. El punto de acceso 1130 puede obtener la segunda clave pública de cliente (en un tercer mensaje) 1116 del segundo dispositivo cliente 1120 y proporcionar la segunda clave pública de cliente (en un cuarto mensaje 1126) al primer dispositivo cliente 1110. En otro modo de realización, el punto de acceso 1130 puede estar configurado para generar una o más claves públicas de cliente efímeras y proporcionárselas al primer y segundo dispositivos cliente 1110, 1120. Por ejemplo, el punto de acceso 1130 puede generar una primera clave pública de cliente y enviar la primera clave pública de cliente al segundo dispositivo cliente 1120. El punto de acceso 1130 puede generar una segunda clave pública de cliente y enviar la segunda clave pública de cliente al primer dispositivo cliente 1110. Cualquiera, o ambas, de la primera clave pública de cliente y la segunda clave pública de cliente pueden ser claves públicas de cliente efímeras generadas por el punto de acceso 1130.

[92] El primer dispositivo cliente 1110 o bien el segundo dispositivo cliente 1120 puede iniciar el proceso de registro 1131 basándose en las claves públicas de cliente recibidas desde el punto de acceso 1130. En un ejemplo, el primer dispositivo cliente 1110 puede iniciar el proceso de autenticación enviando un mensaje de petición de autenticación 1134 al segundo dispositivo cliente 1120. El mensaje de petición de autenticación 1134 puede incluir un primer *nonce* y, opcionalmente, puede incluir información adicional relativa al primer dispositivo cliente 1110. El segundo dispositivo cliente 1120 puede generar un segundo *nonce*, y usar el segundo *nonce*, el primer *nonce* y la primera clave pública de cliente para determinar una clave compartida. En el mensaje de respuesta de autenticación 1132, el segundo dispositivo cliente 1120 puede incluir el segundo *nonce*, así como un MAC basándose al menos en parte en la clave compartida.

[93] El primer dispositivo cliente 1110 puede usar el primer *nonce*, el segundo *nonce* y la segunda clave pública de cliente 1126 para determinar la misma clave compartida. La clave compartida se verifica generando un MAC de verificación y comparando el MAC de verificación con el MAC recibido.

[94] Después del registro y la autenticación, el segundo dispositivo cliente 1120 o el primer dispositivo cliente 1110 pueden proporcionar datos de configuración 1152 para la conexión inalámbrica de igual a igual. Además, se puede realizar (no mostrada) una autenticación adicional (tal como una negociación en 4 pasos o un establecimiento de PMK).

[95] La **figura 12** es un diagrama de proceso de mensajes 1200 que ilustra la agregación de un nuevo dispositivo configurador 1210 a una red, en la que ya está presente un dispositivo configurador existente 1230. La red incluye un dispositivo de red 1220 que puede proporcionar una clave pública de red 1213, a través de un medio fuera de banda, al nuevo dispositivo configurador 1210. Por ejemplo, el nuevo dispositivo configurador 1210 puede escanear un código QR asociado con el dispositivo de red 1220. El nuevo dispositivo configurador 1210 puede incluir la clave pública de red en un mensaje de registro 1225 para el dispositivo de red 1220. El dispositivo de red 1220 puede determinar que un dispositivo configurador existente ya está presente y puede enviar un mensaje de respuesta 1227 que indica que ya se ha aprovisionado un dispositivo configurador existente 1230. En un modo de realización, el mensaje de respuesta 1227 puede proporcionar un indicador (por ejemplo, nombre o ubicación) del dispositivo configurador existente 1230. El nuevo dispositivo configurador 1210 puede enviar opcionalmente un acuse de recibo 1229 como respuesta al mensaje de respuesta 1227.

[96] El nuevo dispositivo configurador 1210 puede proporcionar un código QR 1231 e indicar al usuario que escanee el código QR mediante el dispositivo configurador existente 1230. El código QR puede tener una clave pública de dispositivo asociada con el nuevo dispositivo configurador 1210. La clave pública de dispositivo se proporciona al dispositivo configurador existente 1230 (por ejemplo, el dispositivo configurador existente 1230 escanea 1233 el código QR proporcionado por el nuevo dispositivo configurador 1210). El dispositivo configurador

existente 1230 puede proporcionar la clave pública de dispositivo (en un mensaje fiable 1235) al dispositivo de red 1220 usando una relación fiable existente entre el dispositivo configurador existente 1230 y el dispositivo de red 1220. En respuesta a la recepción de la clave pública de dispositivo, el dispositivo de red 1220 puede registrar el nuevo dispositivo configurador 1210 y agregarlo a una lista de dispositivos configuradores.

[97] La **figura 13** es un diagrama conceptual que ilustra listas de claves públicas que diversos dispositivos pueden mantener de acuerdo con un modo de realización de la presente divulgación. En la figura 13, el dispositivo cliente 110 puede tener una memoria 1310 para almacenar las claves públicas asociadas con al menos un dispositivo de red. La memoria 1310 también puede almacenar la clave pública de un dispositivo configurador. En un modo de realización, la memoria 1310 puede almacenar claves públicas para más de un dispositivo de red, tal como cuando se aprovisiona el dispositivo cliente 110 para acceder a diferentes redes basándose en cobertura o selección del usuario.

[98] El dispositivo configurador 130 puede tener memoria 1330 para almacenar claves públicas para una lista de dispositivos cliente que se aprovisionan para la red. La lista de dispositivos cliente se puede compartir con un nuevo dispositivo de red (no mostrado) cuando se agrega un nuevo dispositivo de red a la red. La memoria 1330 también puede almacenar las claves públicas para una lista de dispositivos de red asociados con la red. Las claves públicas para la lista de dispositivos de red se pueden usar para verificar peticiones de un dispositivo de red.

[99] El dispositivo de red 120 puede tener memoria 1320 para almacenar claves públicas asociadas con una lista de dispositivos cliente y claves públicas para una lista de dispositivos configuradores. Cuando se agrega un nuevo dispositivo de red a la red, las claves públicas para la lista de dispositivos cliente pueden compartirse con el nuevo dispositivo de red de tal manera que el nuevo dispositivo de red pueda registrar automáticamente los dispositivos cliente. Las claves públicas para la lista de dispositivos configuradores también pueden compartirse con un nuevo dispositivo de red de tal manera que el nuevo dispositivo de red pueda verificar peticiones de registro recibidas por dispositivos configuradores de la red.

[100] Utilizando los ejemplos de la figura 13, se puede entender que las listas (y claves públicas asociadas) se pueden usar para administrar el acceso en una red. Por ejemplo, cuando un usuario hace que un dispositivo cliente se elimine de la lista de dispositivos cliente de un dispositivo configurador, los cambios pueden propagarse a otros dispositivos configuradores y dispositivos de red. Utilizando la figura 13 como ejemplo, el dispositivo configurador 130 puede enviar un mensaje al dispositivo de red 120 para hacer que el dispositivo de red 120 elimine la clave pública para el dispositivo cliente 110 de la lista de dispositivos cliente en la memoria 1320. En consecuencia, el dispositivo cliente 110 no estaría aprovisionado para la red.

[101] Las figuras 1-13 y las operaciones descritas en el presente documento son ejemplos que pretenden facilitar la comprensión de diversos modos de realización y no deben usarse para limitar el alcance de las reivindicaciones. Los modos de realización pueden realizar operaciones adicionales, menos operaciones, operaciones en paralelo o en un orden diferente y algunas operaciones de manera diferente. Si bien la presente divulgación enumera varios modos de realización, se consideran modos de realización adicionales dentro del alcance de esta divulgación. Por ejemplo, en un modo de realización, un procedimiento para autenticar un dispositivo cliente con un dispositivo de red comprende facilitar, a través de un dispositivo configurador, una autenticación entre el dispositivo cliente y el dispositivo de red, estando basada la autenticación al menos en parte en una clave pública de cliente del dispositivo cliente compartida desde el dispositivo cliente con el dispositivo de red a través del dispositivo configurador, usando el dispositivo configurador comunicaciones fuera de banda para obtener la clave pública de cliente.

[102] Como apreciará un experto en la materia, los aspectos de la presente divulgación pueden realizarse como un sistema, procedimiento o producto de programa informático. En consecuencia, los aspectos de la presente divulgación pueden adoptar la forma de una realización enteramente de hardware, una realización de software (incluyendo firmware, software residente, microcódigo, etc.) o una realización que combina aspectos de software y hardware, todas las cuales pueden denominarse en general "circuito", "unidad" o "sistema" en el presente documento. Además, aspectos de la presente divulgación pueden adoptar la forma de un producto de programa informático realizado en uno o más medios legibles por ordenador que tienen código de programa legible por ordenador realizado en los mismos.

[103] Se puede usar cualquier combinación de uno o más medios legibles por ordenador, con la única excepción de una señal de propagación transitoria. El medio legible por ordenador puede ser un medio de almacenamiento legible por ordenador. Un medio de almacenamiento legible por ordenador puede ser, por ejemplo, pero sin estar limitado a, un sistema, aparato o dispositivo electrónico, magnético, óptico, electromagnético, de infrarrojos o semiconductores o cualquier combinación adecuada de los anteriores. Ejemplos más específicos (una lista no exhaustiva) del medio de almacenamiento legible por ordenador incluirían los siguientes: una conexión eléctrica que tiene uno o más hilos, un disquete de ordenador portátil, un disco duro, una memoria de acceso aleatorio (RAM), una memoria de solo lectura (ROM), una memoria de solo lectura programable y borrable (EPROM o memoria *flash*), una fibra óptica, una memoria de solo lectura de disco compacto (CD-ROM) portátil, un dispositivo de almacenamiento óptico, un dispositivo de almacenamiento magnético o cualquier combinación adecuada de los anteriores. En el contexto de este documento, un medio de almacenamiento legible por ordenador puede ser

cualquier medio tangible que pueda contener o almacenar un programa para su uso por, o en conexión con, un sistema, aparato o dispositivo de ejecución de instrucciones.

[104] El código de programa informático realizado en un medio legible por ordenador para llevar a cabo operaciones para aspectos de la presente divulgación puede escribirse en cualquier combinación de uno o más lenguajes de programación, incluyendo un lenguaje de programación orientado a objetos tal como Java, Smalltalk, C++ o similares, y lenguajes de programación procedurales convencionales, tales como el lenguaje de programación "C" o lenguajes de programación similares. El código de programa puede ejecutarse completamente en el ordenador del usuario, parcialmente en el ordenador del usuario, como un paquete de software autónomo, parcialmente en el ordenador del usuario y parcialmente en un ordenador remoto, o completamente en el ordenador o servidor remoto. En el último caso, el ordenador remoto puede estar conectado al ordenador del usuario a través de cualquier tipo de red, incluyendo una red de área local (LAN) o una red de área amplia (WAN), o la conexión puede realizarse con un ordenador externo (por ejemplo, a través de Internet usando un proveedor de servicios de Internet).

[105] Aspectos de la presente divulgación se describen con referencia a ilustraciones de diagramas de flujo y/o diagramas de bloques de procedimientos, aparatos (sistemas) y productos de programa informático de acuerdo con modos de realización de la presente divulgación. Debe entenderse que cada bloque de las ilustraciones de diagramas de flujo y/o diagramas de bloques, y combinaciones de bloques en las ilustraciones de diagramas de flujo y/o diagramas de bloques, pueden implementarse mediante instrucciones de programa informático. Estas instrucciones de programa informático se pueden proporcionar a un procesador de ordenador de propósito general, ordenador de propósito especial u otro aparato de procesamiento de datos programable para producir una máquina, de tal manera que las instrucciones, que se ejecutan a través del procesador del ordenador u otro aparato de procesamiento de datos programable, creen medios para implementar las funciones/actos especificados en el bloque o bloques del diagrama de flujo y/o diagrama de bloques.

[106] Estas instrucciones de programa informático también pueden almacenarse en un medio legible por ordenador que puede dirigir un ordenador, otro aparato de procesamiento de datos programable u otros dispositivos para que funcione de una manera particular, de tal manera que las instrucciones almacenadas en el medio legible por ordenador produzcan un artículo de fabricación que incluya instrucciones que implementen la función/acto especificados en el bloque o bloques del diagrama de flujo y/o diagrama de bloques. Las instrucciones de programa informático también pueden cargarse en un ordenador, otro aparato de procesamiento de datos programable u otros dispositivos para hacer que se realicen una serie de etapas operativas en el ordenador, otros aparatos programables u otros dispositivos para producir un proceso implementado por ordenador de tal manera que las instrucciones que se ejecutan en el ordenador u otro aparato programable proporcionen procesos para implementar las funciones/actos especificados en el bloque o bloques del diagrama de flujo y/o diagrama de bloques.

[107] La **figura 14** es un diagrama de bloques de ejemplo de un modo de realización de un dispositivo electrónico 1400 capaz de implementar diversos modos de realización de la presente divulgación. En algunas implementaciones, el dispositivo electrónico 1400 puede ser un dispositivo electrónico tal como un ordenador portátil, una tableta, un teléfono móvil, una consola de juegos u otro sistema electrónico. El dispositivo electrónico 1400 incluye un procesador 1402 (que incluye posiblemente múltiples procesadores, múltiples núcleos, múltiples nodos y/o que implementa múltiples hilos, etc.). El dispositivo electrónico 1400 incluye una memoria 1406. La memoria 1406 puede ser una memoria de sistema (por ejemplo, una o más de entre una memoria caché, una SRAM, una DRAM, una RAM sin condensadores, una RAM con dos transistores, una eDRAM, una EDO RAM, una DDR RAM, una EEPROM, una NRAM, una RRAM, una SONOS, una PRAM, etc.) o una cualquiera o más de los posibles modos de realización descritos anteriormente de medios legibles por máquina. El dispositivo electrónico 1400 también incluye un bus 1401 (por ejemplo, PCI, ISA, PCI-Express, Hyper-Transport®, InfiniBand®, NuBus, AHB, AXI, etc.). Las una o más interfaces de red electrónicas que pueden ser una interfaz de red inalámbrica (por ejemplo, una interfaz WLAN, una interfaz Bluetooth®, una interfaz WiMAX, una interfaz ZigBee®, una interfaz USB inalámbrica, etc.) o una interfaz de red alámbrica (por ejemplo, una interfaz de comunicación por línea eléctrica, una interfaz Ethernet, etc.). En algunas implementaciones, un dispositivo electrónico 1400 puede admitir múltiples interfaces de red 1404, cada una de las cuales puede estar configurada para acoplar el dispositivo electrónico 1400 a una red de comunicación diferente.

[108] La memoria 1406 realiza la funcionalidad para implementar modos de realización descritos anteriormente. La memoria 1406 puede incluir una o más funcionalidades que facilitan el registro y la autenticación asistidos. Por ejemplo, la memoria 1406 puede implementar uno o más aspectos del dispositivo cliente 110, dispositivo de red 120 o dispositivo configurador 130 descritos anteriormente. La memoria 1406 puede integrar una funcionalidad para implementar los modos de realización descritos en las figuras 1-13 anteriores. En un modo de realización, una memoria 1406 puede incluir una o más funcionalidades que facilitan el envío y la recepción de claves, mensajes de autenticación y similares.

[109] El dispositivo electrónico 1400 también puede incluir una interfaz de sensor 1420, una interfaz de accionador 1430 u otro componente de entrada/salida. En otros modos de realización, el dispositivo electrónico 1400 puede tener otros sensores apropiados (por ejemplo, una cámara, un micrófono, un detector NFC, un escáner de código de barras, etc.) usados para determinar la clave pública de red y/o la clave pública de cliente.

[110] Una cualquiera de estas funcionalidades puede estar implementada parcialmente (o completamente) en hardware y/o en el procesador 1402. Por ejemplo, la funcionalidad puede implementarse con un circuito integrado específico de la aplicación, en lógica implementada en el procesador 1402, en un coprocesador en un dispositivo periférico o tarjeta, etc. Además, las realizaciones pueden incluir menos componentes o componentes adicionales no ilustrados en la figura 14 (por ejemplo, tarjetas de vídeo, tarjetas de audio, interfaces de red adicionales, dispositivos periféricos, etc.). El procesador 1402 y la memoria 1406 pueden estar conectados al bus 1401. Aunque se ilustra conectada al bus 1401, la memoria 1406 puede estar conectada directamente al procesador 1402.

[111] Aunque los modos de realización se describen con referencia a diversas implementaciones y usos, debe entenderse que estos modos de realización son ilustrativos y que el alcance de la presente divulgación no está limitado a los mismos. En general, pueden implementarse técnicas para aprovisionamiento de dispositivos como las descritas en el presente documento, con servicios consistentes con cualquier sistema de hardware o sistemas de hardware. Muchas variaciones, modificaciones, adiciones y mejoras son posibles.

[112] Pueden proporcionarse varias instancias de componentes, operaciones o estructuras descritos en el presente documento con una única instancia. Finalmente, los límites entre varios componentes, operaciones y medios de almacenamiento de datos son en cierto modo arbitrarios, y operaciones particulares se ilustran en el contexto de configuraciones ilustrativas específicas. Pueden concebirse otras asignaciones de funcionalidad, las cuales pueden estar dentro del alcance de la presente divulgación. En general, las estructuras y la funcionalidad presentadas como componentes independientes en las configuraciones a modo de ejemplo pueden implementarse como una estructura o componente combinados. Asimismo, las estructuras y la funcionalidad presentadas como un único componente pueden implementarse como componentes individuales.

REIVINDICACIONES

1. Un procedimiento realizado por un dispositivo configurador (130) para registro de un dispositivo cliente (110) con una red, comprendiendo el procedimiento:

establecer una relación de confianza (225) con un dispositivo de red (120) de la red;

determinar una clave pública de cliente asociada con el dispositivo cliente antes de un procedimiento de registro entre el dispositivo cliente y el dispositivo de red; y

enviar, desde el dispositivo configurador al dispositivo de red de acuerdo con la relación de confianza, la clave pública de cliente para facilitar el procedimiento de registro, en el que el procedimiento de registro comprende al menos una primera autenticación entre el dispositivo de red y el dispositivo cliente basada, al menos en parte, en la clave pública de cliente.

2. El procedimiento, según la reivindicación 1, que comprende además:

enviar, desde el dispositivo configurador o el dispositivo de red al dispositivo cliente, una clave pública de red asociada con el dispositivo de red, en el que la primera autenticación se basa además, al menos en parte, en la clave pública de red.

3. El procedimiento, según la reivindicación 1, en el que establecer la relación de confianza comprende:

determinar una clave pública de red asociada con el dispositivo de red;

enviar una clave pública de configurador al dispositivo de red, correspondiendo la clave pública de configurador a una clave privada de configurador; y

determinar una clave de relación de confianza asociada con la relación de confianza basándose, al menos en parte, en la clave pública de red y la clave privada de configurador;

en el que determinar la clave pública de red asociada con el dispositivo de red comprende preferentemente:

recibir la clave pública de red a través de una conexión segura con el dispositivo de red, o

determinar la clave pública de red a través de una conexión fuera de banda con el dispositivo de red que es diferente de una conexión que el dispositivo cliente establecerá con el dispositivo de red, o

detectar la clave pública de red usando al menos un miembro del grupo que consiste en una cámara, un micrófono, un detector de luz, un sensor y una interfaz de radiofrecuencia de corto alcance del dispositivo configurador, en el que detectar la clave pública de la red usando la cámara preferentemente comprende usar la cámara para detectar una imagen asociada con el dispositivo de red, en el que al menos una parte de la imagen incluye la clave pública de red;

en el que establecer la relación de confianza comprende preferentemente recibir un anuncio de servicio de compatibilidad con configurador desde el dispositivo de red antes de determinar la clave pública de red asociada con el dispositivo de red.

4. El procedimiento, según la reivindicación 3, que comprende además:

encriptar la clave pública de cliente con la clave de relación de confianza antes de enviar la clave pública de cliente desde el dispositivo configurador al dispositivo de red.

5. El procedimiento, según la reivindicación 1, en el que determinar la clave pública de cliente asociada con el dispositivo cliente comprende:

detectar la clave pública de cliente usando al menos un miembro del grupo que consiste en una cámara, un micrófono, un detector de luz, un sensor y una interfaz de radiofrecuencia de corto alcance del dispositivo configurador;

en el que detectar la clave pública de cliente usando la cámara comprende preferentemente usar la cámara para detectar una imagen asociada con el dispositivo cliente.

6. El procedimiento, según la reivindicación 1, en el que enviar la clave pública de cliente asociada con el dispositivo cliente comprende:

enviar un mensaje de petición al dispositivo de red;

recibir un *nonce* desde el dispositivo de red; y

enviar un mensaje de registro al dispositivo de red, incluyendo el mensaje de registro la clave pública de cliente y una firma de configurador obtenida, al menos en parte, del *nonce* y una clave privada de configurador, en el que la firma del configurador proporciona una segunda autenticación al dispositivo de red de que el dispositivo configurador está autorizado para enviar el mensaje de registro;

en el que la firma de configurador se obtiene preferentemente del *nonce* y de una clave privada de configurador o se basa, al menos en parte, en una clave de relación de confianza asociada con la relación de confianza;

en el que el procedimiento comprende preferentemente además:

recibir una clave de registro desde el dispositivo de red; y

enviar la clave de registro al dispositivo cliente, en el que la clave de registro se usa con la clave pública de cliente para la primera autenticación entre el dispositivo de red y el dispositivo cliente.

7. El procedimiento, según la reivindicación 1, que comprende además:

enviar datos de configuración desde el dispositivo configurador al dispositivo de red después de establecer la relación de confianza.

8. El procedimiento, según la reivindicación 1, que comprende además:

enviar datos de configuración desde el dispositivo configurador al dispositivo cliente para ayudar al dispositivo cliente en la asociación con el dispositivo de red;

en el que enviar los datos de configuración comprende preferentemente transmitir un primer mensaje en un canal predeterminado accesible por el dispositivo cliente;

en el que el primer mensaje incluye preferentemente información de identidad basada, al menos en parte, en la clave pública de cliente o bien en una clave pública de red asociada con el dispositivo de red.

9. El procedimiento, según la reivindicación 1, en el que el dispositivo cliente es un primer dispositivo cliente, el dispositivo de red es un segundo dispositivo cliente y el dispositivo configurador es un punto de acceso; o

en el que el dispositivo de red es un punto de acceso de la red, y en el que el dispositivo configurador está asociado con el punto de acceso.

10. Un procedimiento realizado por un dispositivo de red (120) para registro de un dispositivo cliente (110) en una red, comprendiendo el procedimiento:

establecer, en el dispositivo de red, una relación de confianza (225) con un dispositivo configurador (130)

recibir, desde el dispositivo configurador de acuerdo con la relación de confianza, una clave pública de cliente asociada con el dispositivo cliente antes de un procedimiento de registro entre el dispositivo cliente y el dispositivo de red; y

usar la clave pública de cliente para el procedimiento de registro, en el que el procedimiento de registro comprende al menos una primera autenticación entre el dispositivo de red y el dispositivo cliente basada, al menos en parte, en la clave pública de cliente.

11. Un procedimiento realizado por un dispositivo cliente (110) para registro en una red, comprendiendo el procedimiento:

proporcionar, a un dispositivo configurador (130) que tiene una relación de confianza (225) con un dispositivo de red (120) de la red, una clave pública de cliente asociada con el dispositivo cliente antes de un procedimiento de registro entre el dispositivo cliente y el dispositivo de red;

recibir, desde el dispositivo configurador, un primer *nonce* y una clave pública de red asociada con el dispositivo de red;

generar un segundo *nonce*;

determinar una clave compartida basándose, al menos en parte, en el primer *nonce*, el segundo *nonce*, la clave pública de red y una clave privada de cliente asociada con el dispositivo cliente, en el que la clave privada de cliente corresponde a la clave pública de cliente; y

usar la clave compartida para el procedimiento de registro, en el que el procedimiento de registro comprende al menos una primera autenticación entre el dispositivo de red y el dispositivo cliente basada, al menos en parte, en la clave compartida.

12. Un dispositivo configurador adaptado para realizar un procedimiento de acuerdo con cualquiera de las reivindicaciones anteriores 1-9.

13. Un dispositivo de red adaptado para realizar un procedimiento de acuerdo con la reivindicación 10.

14. Un dispositivo cliente adaptado para realizar un procedimiento de acuerdo con la reivindicación 11.

15. Un producto de programa informático que comprende instrucciones para implementar un procedimiento de acuerdo con cualquiera de las reivindicaciones anteriores 1-9, 10 y/u 11.

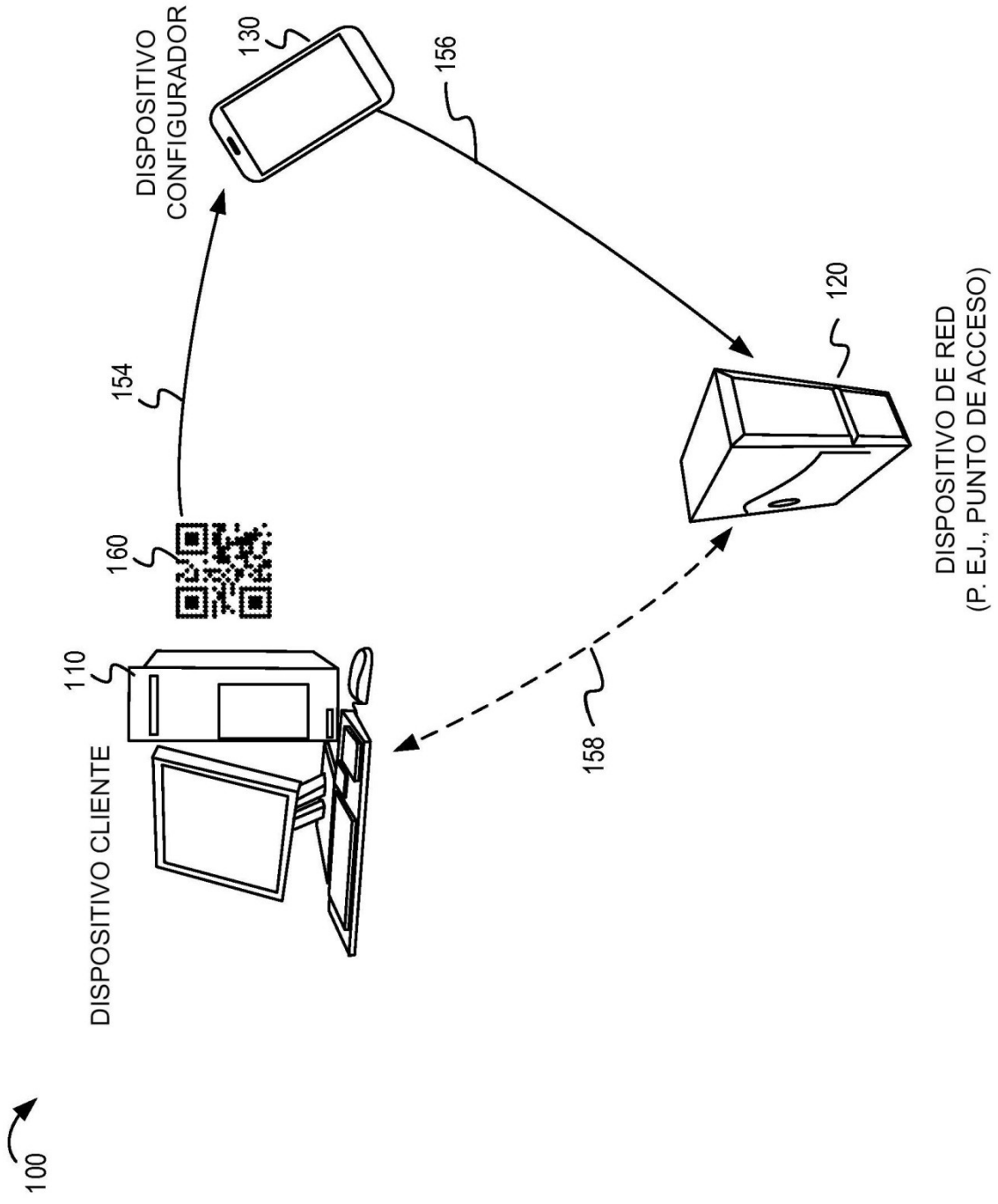
100
DISPOSITIVO CLIENTE
110
DISPOSITIVO CONFIGURADOR
130
DISPOSITIVO DE RED
(P. EJ., PUNTO DE ACCESO)
120
154
156
158
160

FIG. 1

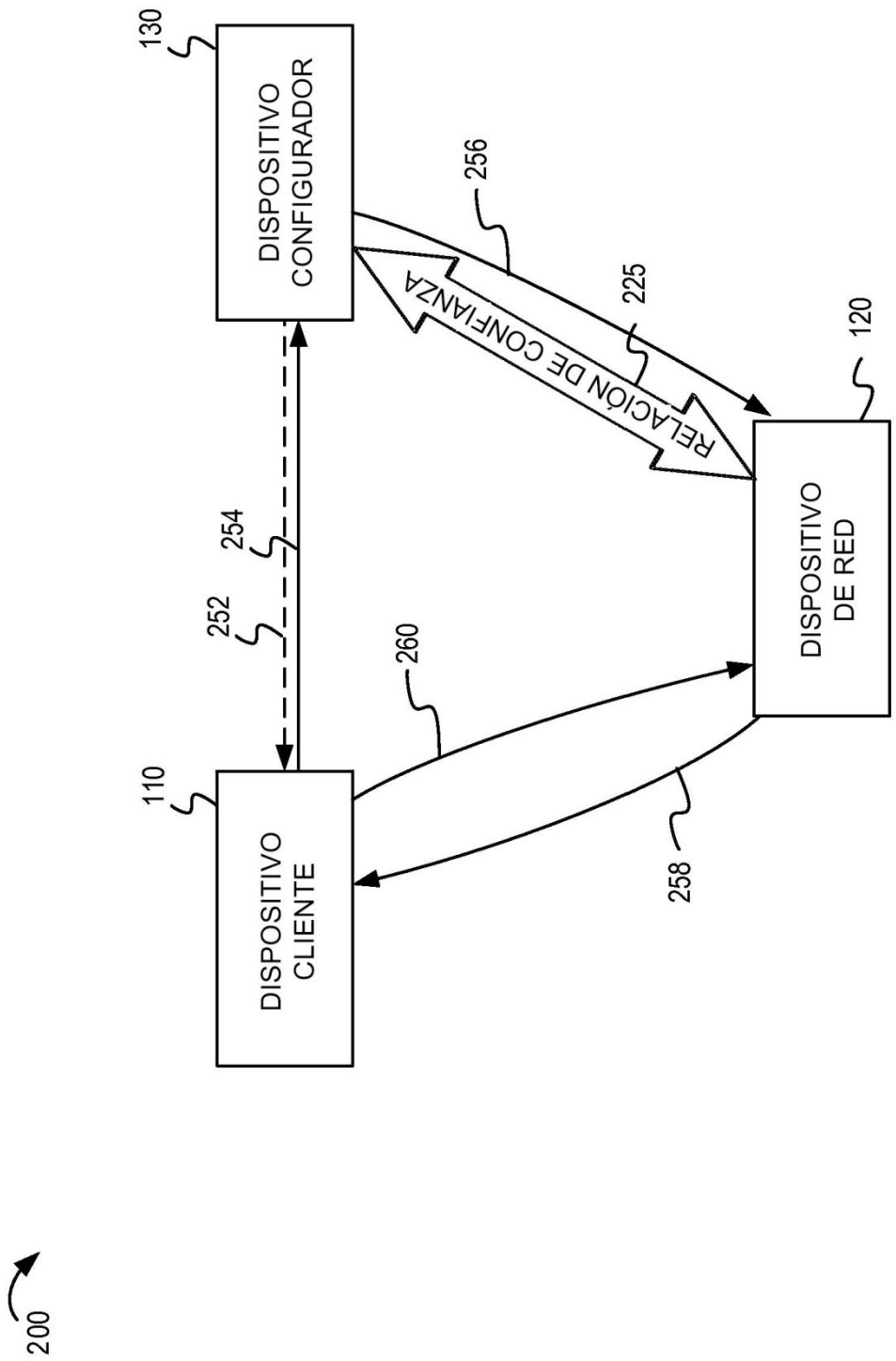
200
130
DISPOSITIVO CONFIGURADOR
256
225
RELACIÓN DE CONFIANZA
120
DISPOSITIVO DE RED
254
252
260
110
DISPOSITIVO CLIENTE
258

FIG. 2

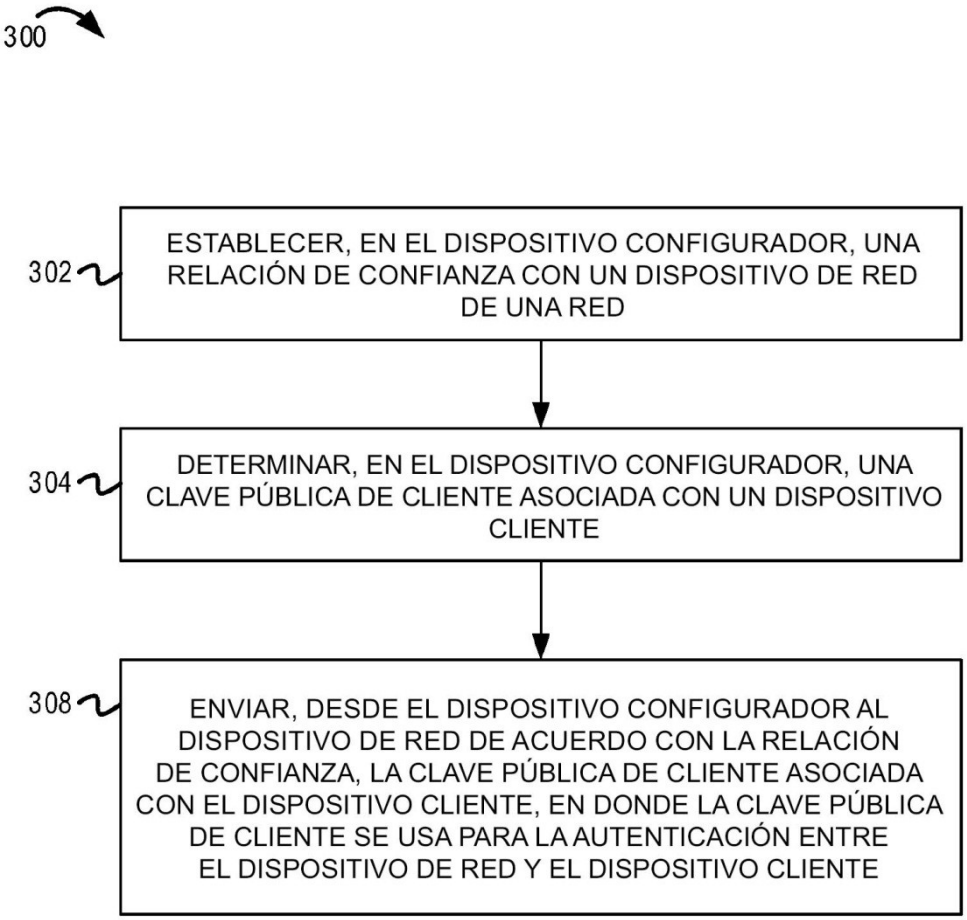
300
302
ESTABLECER, EN EL DISPOSITIVO CONFIGURADOR, UNA RELACIÓN DE CONFIANZA CON UN DISPOSITIVO DE RED DE UNA RED
304
DETERMINAR, EN EL DISPOSITIVO CONFIGURADOR, UNA CLAVE PÚBLICA DE CLIENTE ASOCIADA CON UN DISPOSITIVO CLIENTE
308
ENVIAR, DESDE EL DISPOSITIVO CONFIGURADOR AL DISPOSITIVO DE RED DE ACUERDO CON LA RELACIÓN DE CONFIANZA, LA CLAVE PÚBLICA DE CLIENTE ASOCIADA CON EL DISPOSITIVO CLIENTE, EN DONDE LA CLAVE PÚBLICA DE CLIENTE SE USA PARA LA AUTENTICACIÓN ENTRE EL DISPOSITIVO DE RED Y EL DISPOSITIVO CLIENTE

FIG. 3

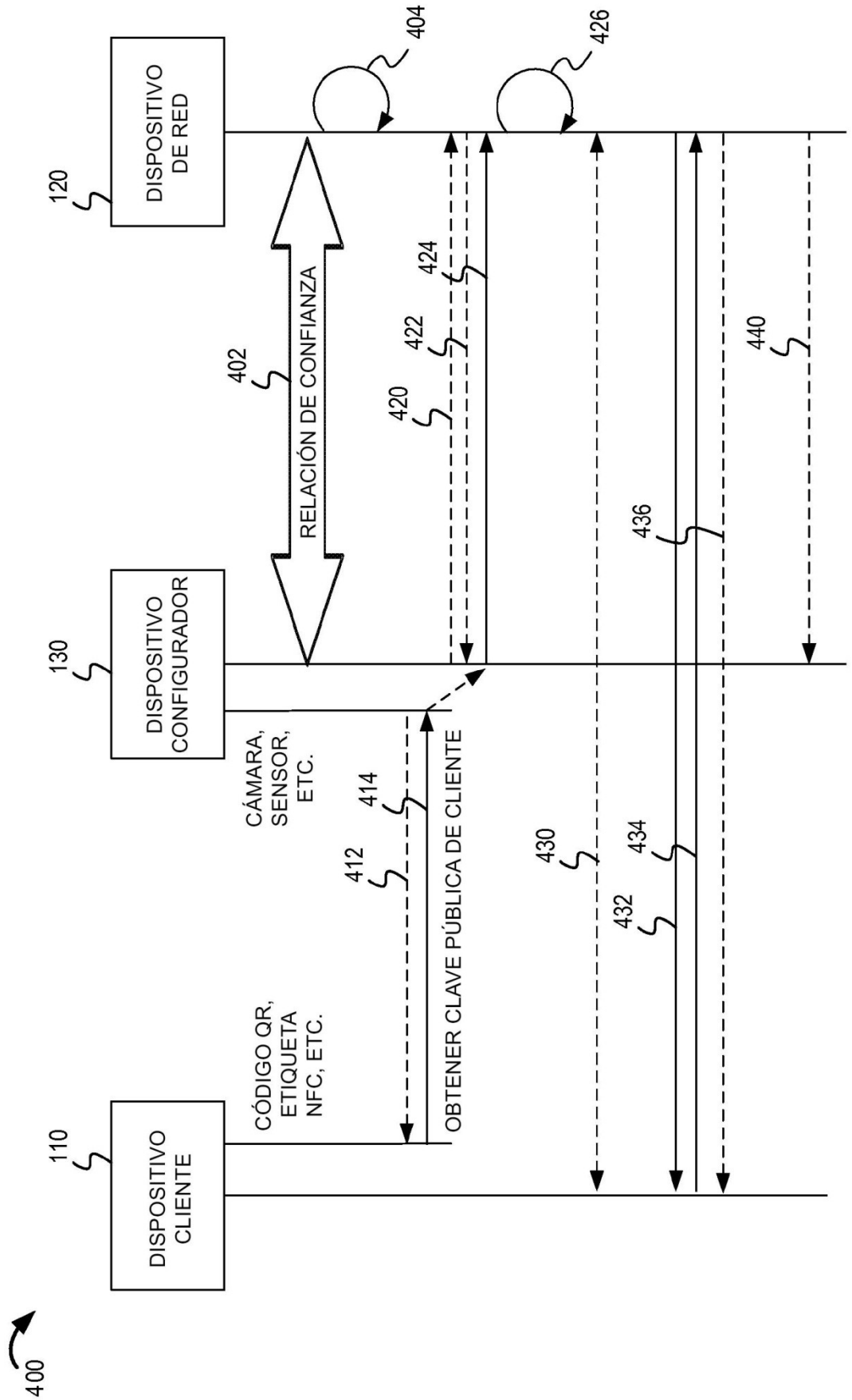
400
DISPOSITIVO CLIENTE
110
DISPOSITIVO CONFIGURADOR
130
DISPOSITIVO DE RED
120
CÓDIGO QR, ETIQUETA NFC, ETC.
CÁMARA, SENSOR, ETC.
RELACIÓN DE CONFIANZA
402
404
412
414
420
422
424
426
430
432
434
436
440
OBTENER CLAVE PÚBLICA DE CLIENTE

FIG. 4

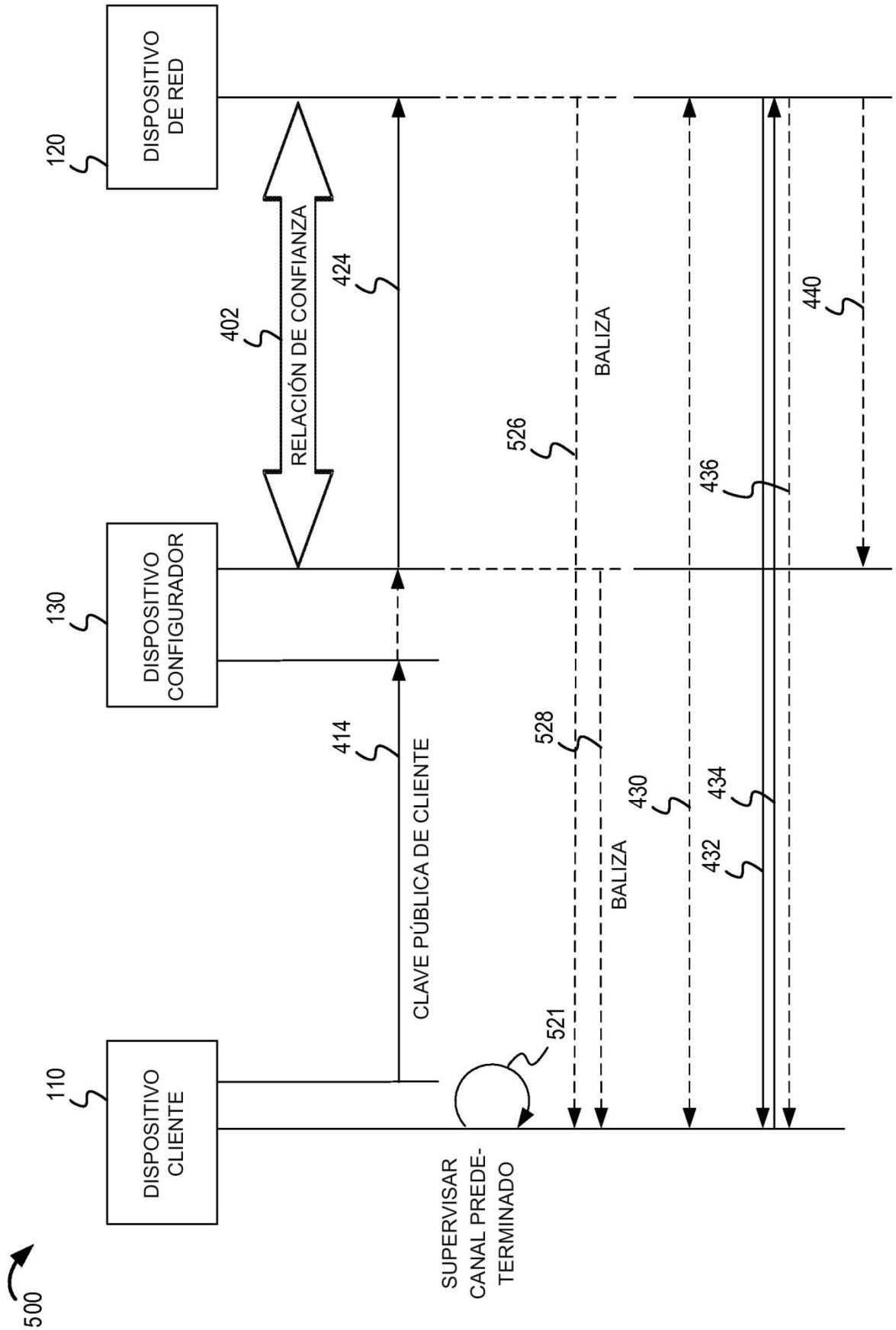
500
DISPOSITIVO CLIENTE
110
DISPOSITIVO CONFIGURADOR
130
DISPOSITIVO DE RED
120
SUPERVISAR CANAL PREDE-TERMINADO
CLAVE PÚBLICA DE CLIENTE
414
RELACIÓN DE CONFIANZA
402
424
521
526
528
BALIZA
BALIZA
430
432
434
436
440

FIG. 5

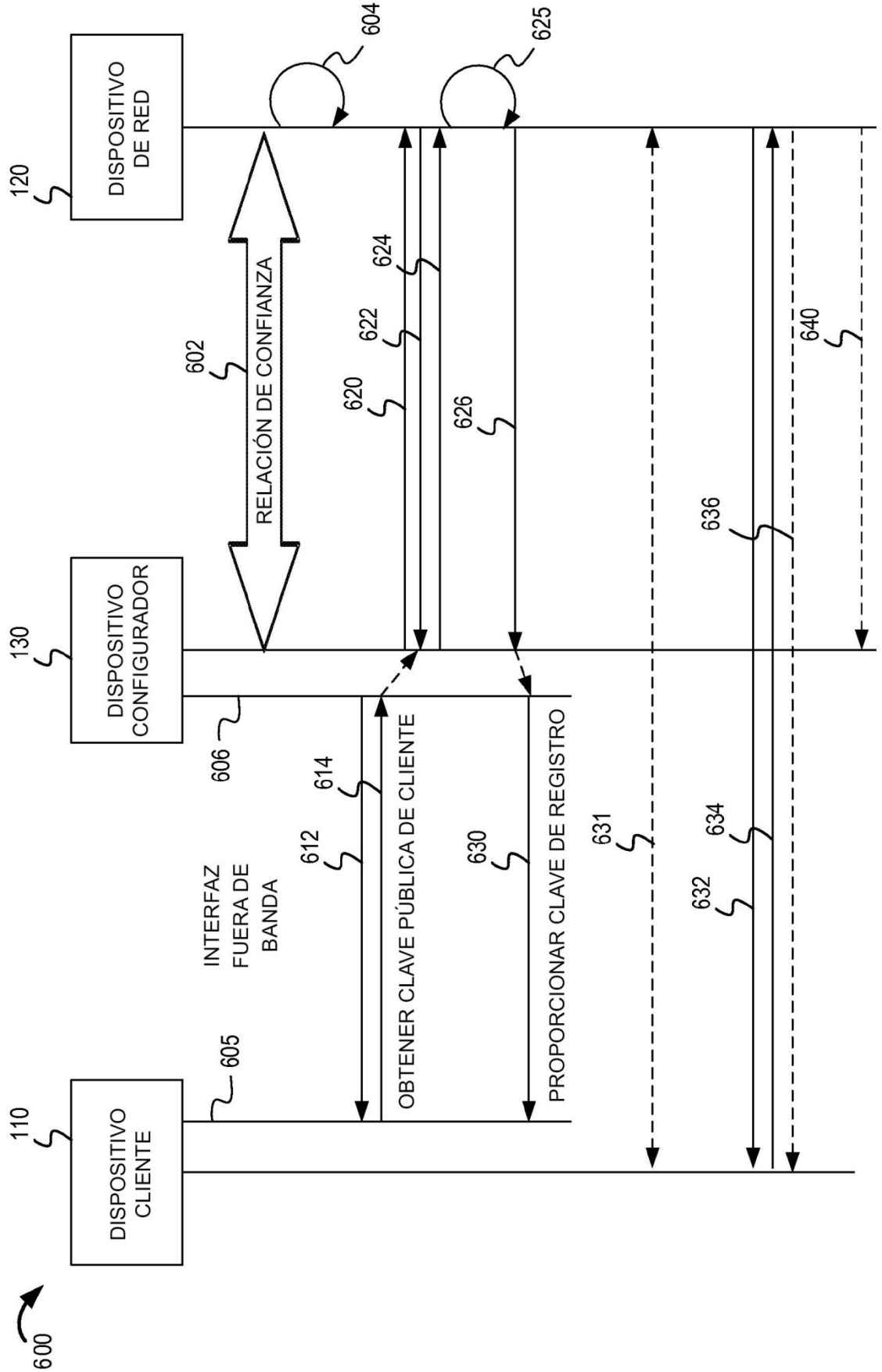
600
DISPOSITIVO CLIENTE
110
DISPOSITIVO CONFIGURADOR
130
DISPOSITIVO DE RED
120
INTERFAZ FUERA DE BANDA
605
606
RELACIÓN DE CONFIANZA
602
604
625
620
622
624
626
OBTENER CLAVE PÚBLICA DE CLIENTE
612
614
PROPORCIONAR CLAVE DE REGISTRO
630
631
632
634
636
640

FIG. 6

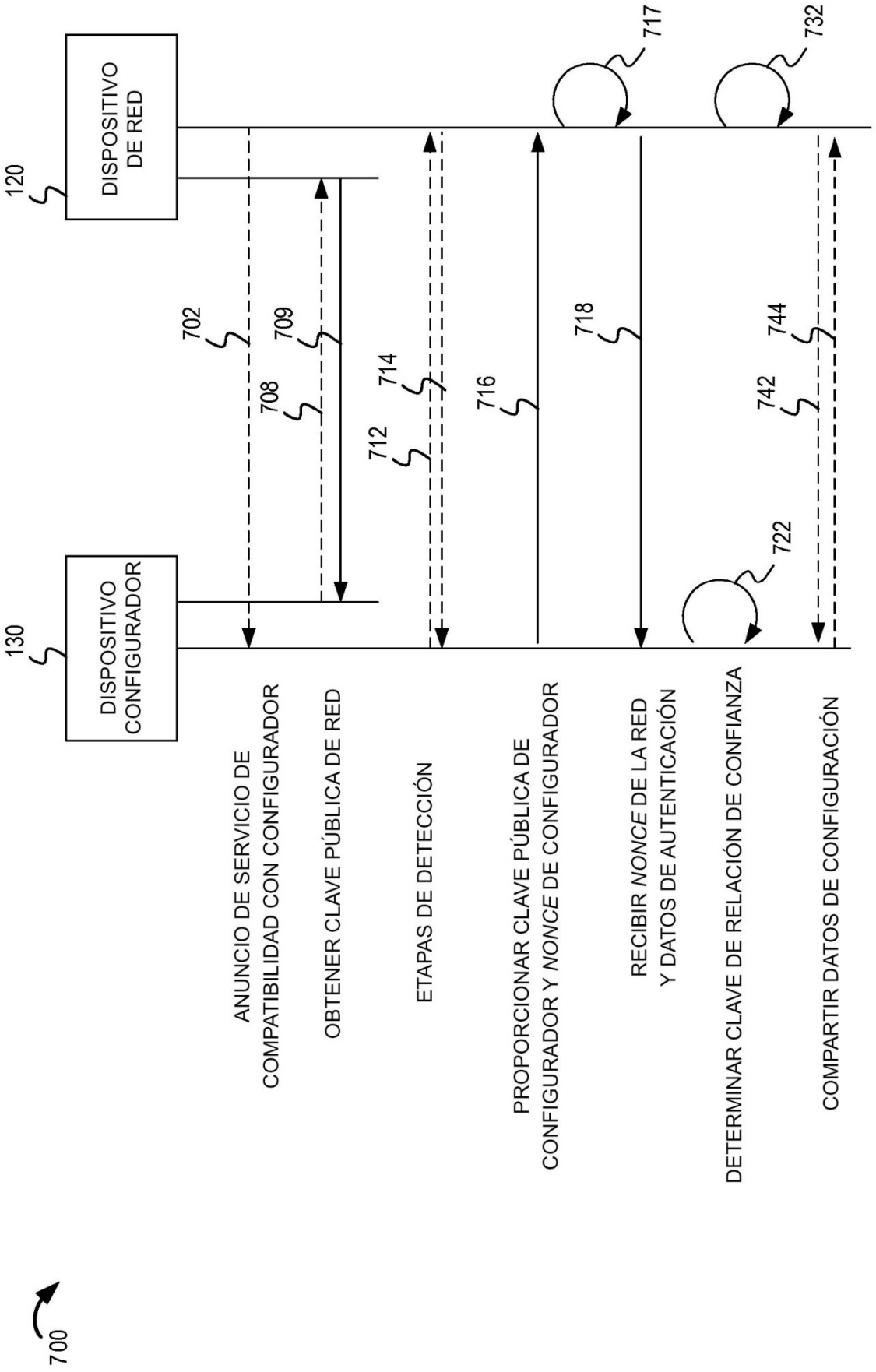
700
130
DISPOSITIVO CONFIGURADOR
120
DISPOSITIVO DE RED
ANUNCIO DE SERVICIO DE COMPATIBILIDAD CON CONFIGURADOR
OBTENER CLAVE PÚBLICA DE RED
ETAPAS DE DETECCIÓN
PROPORCIONAR CLAVE PÚBLICA DE CONFIGURADOR Y *NONCE* DE CONFIGURADOR
RECIBIR *NONCE* DE LA RED Y DATOS DE AUTENTICACIÓN
DETERMINAR CLAVE DE RELACIÓN DE CONFIANZA
COMPARTIR DATOS DE CONFIGURACIÓN
702
708
709
712
714
716
717
718
722
732
742
744

FIG. 7

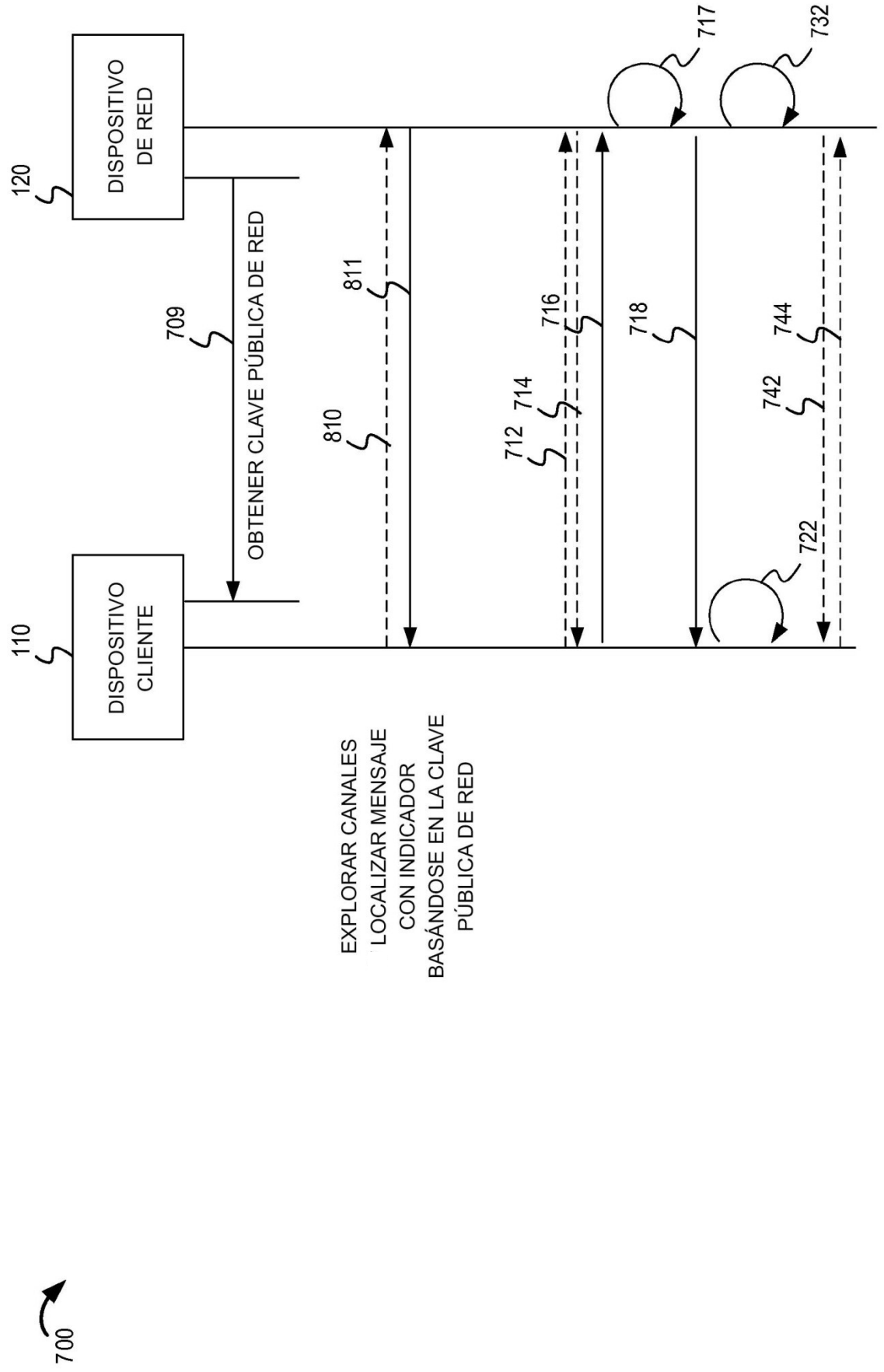
700
DISPOSITIVO CLIENTE
110
DISPOSITIVO DE RED
120
OBTENER CLAVE PÚBLICA DE RED
709
EXPLORAR CANALES
LOCALIZAR MENSAJE
CON INDICADOR
BASÁNDOSE EN LA CLAVE
PÚBLICA DE RED
810
811
712
714
716
718
717
722
742
744
732

FIG. 8

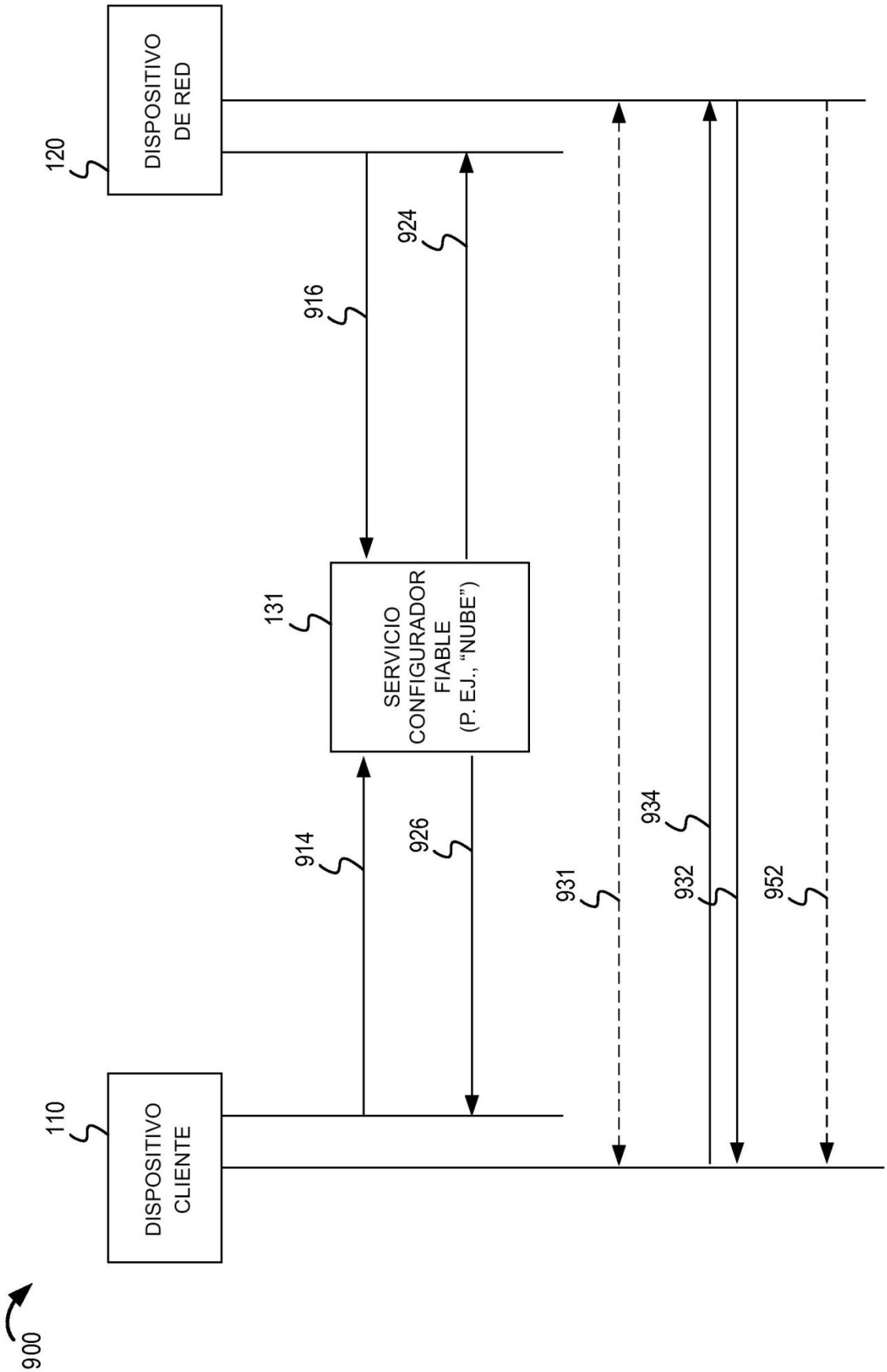
DISPOSITIVO DE RED
120
DISPOSITIVO CLIENTE
110
SERVICIO CONFIGURADOR FIABLE (P. EJ., "NUBE")
131
916
924
914
926
931
934
932
952
900

FIG. 9

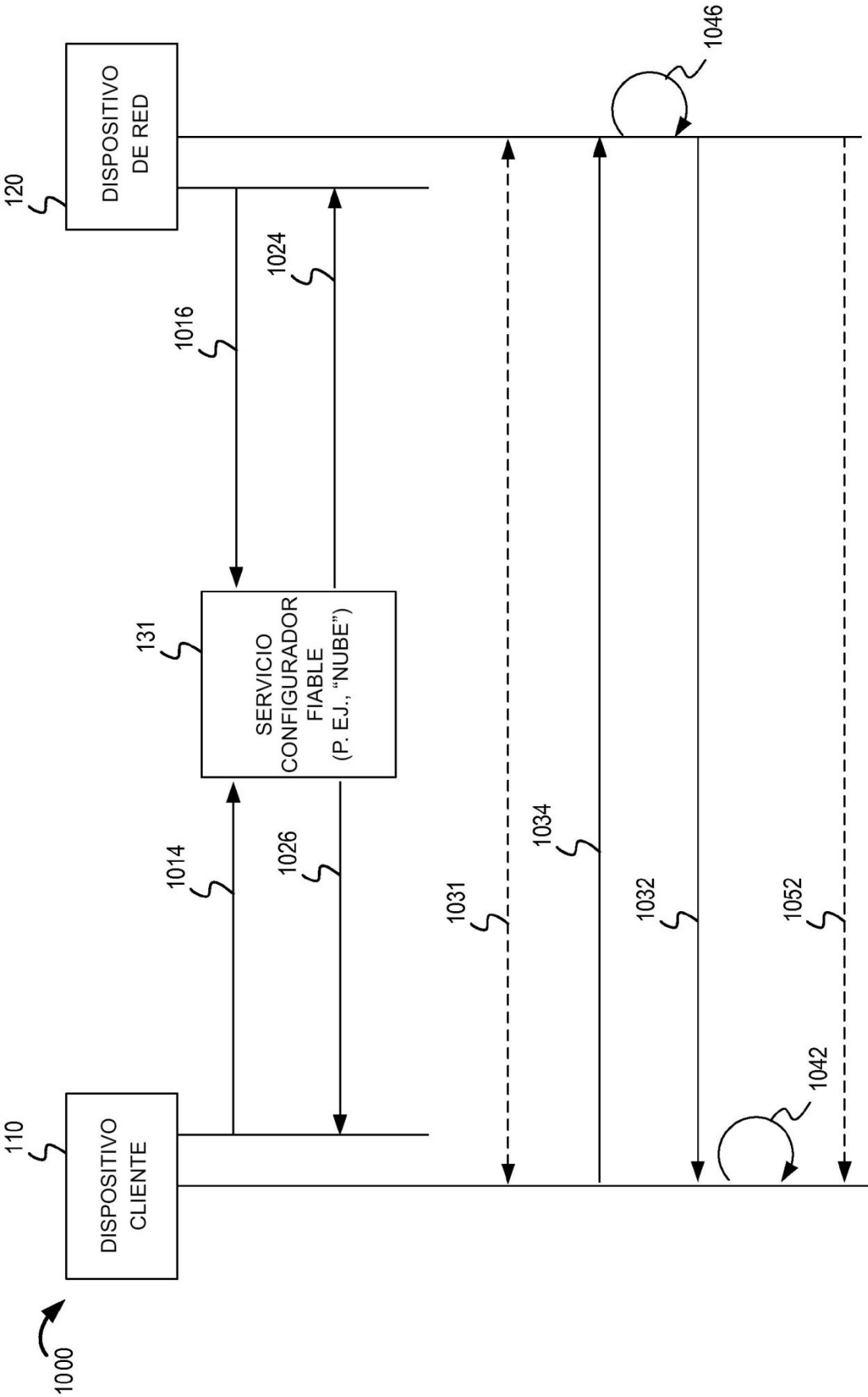
1000
110
DISPOSITIVO CLIENTE
120
DISPOSITIVO DE RED
131
SERVICIO CONFIGURADOR FIABLE (P. EJ., "NUBE")
1014
1016
1024
1026
1031
1032
1034
1042
1046
1052

FIG. 10

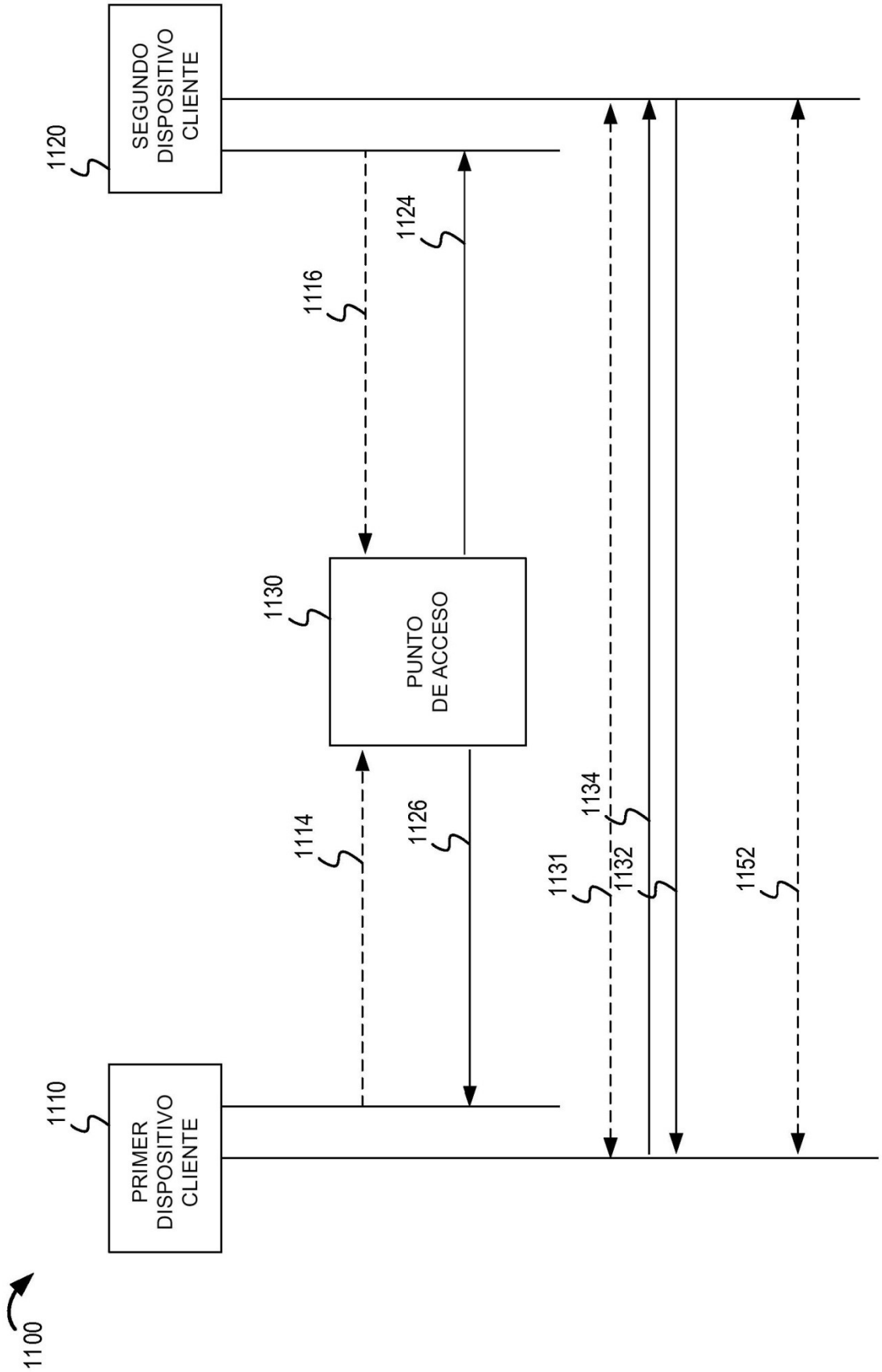
1100
PRIMER DISPOSITIVO CLIENTE
1110
SEGUNDO DISPOSITIVO CLIENTE
1120
PUNTO DE ACCESO
1130
1114
1116
1124
1126
1131
1132
1134
1152

FIG. 11

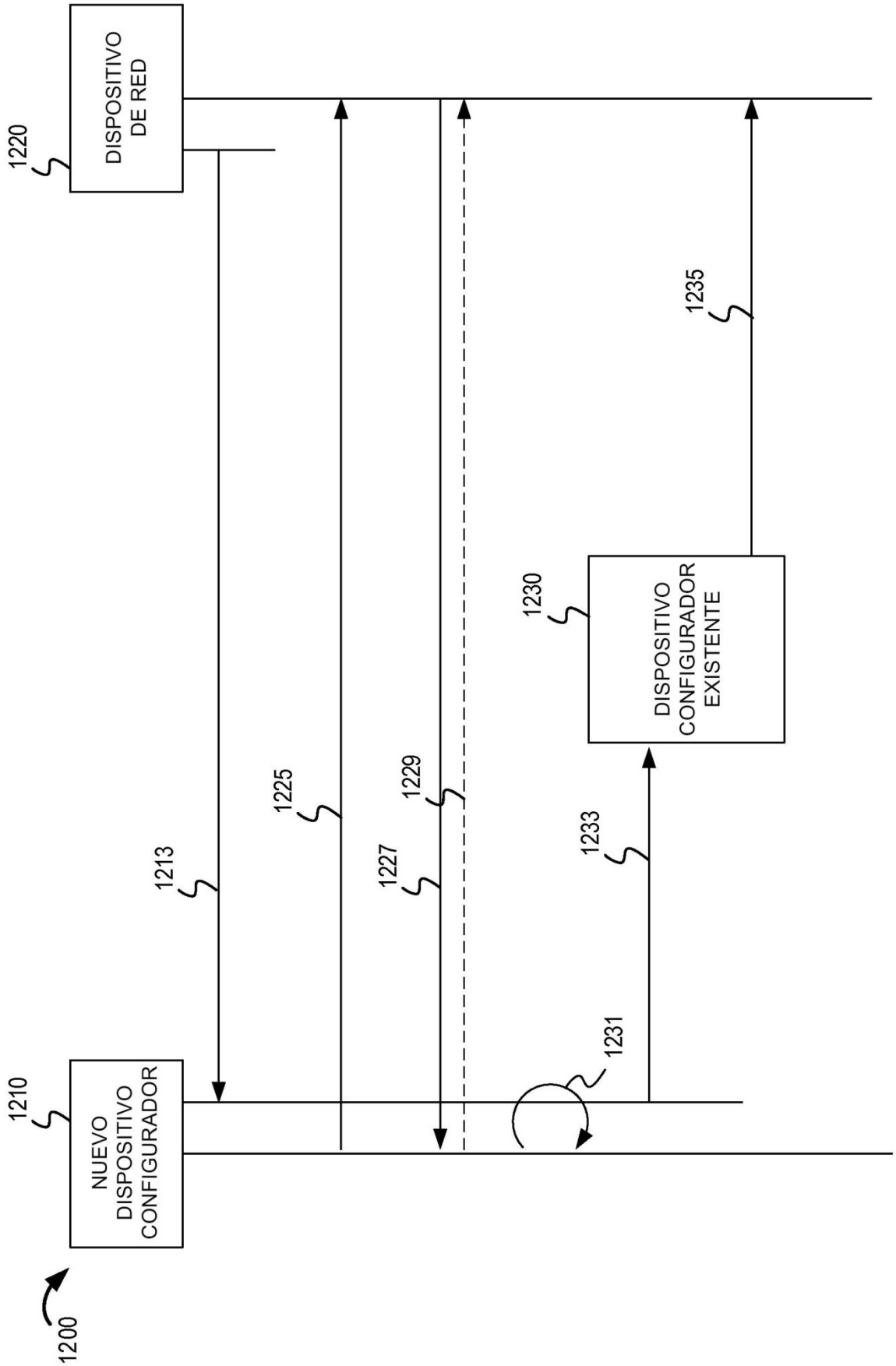
1200
1210
NUEVO DISPOSITIVO CONFIGURADOR
1220
DISPOSITIVO DE RED
1213
1225
1227
1229
1231
1233
1230
DISPOSITIVO CONFIGURADOR EXISTENTE
1235

FIG. 12

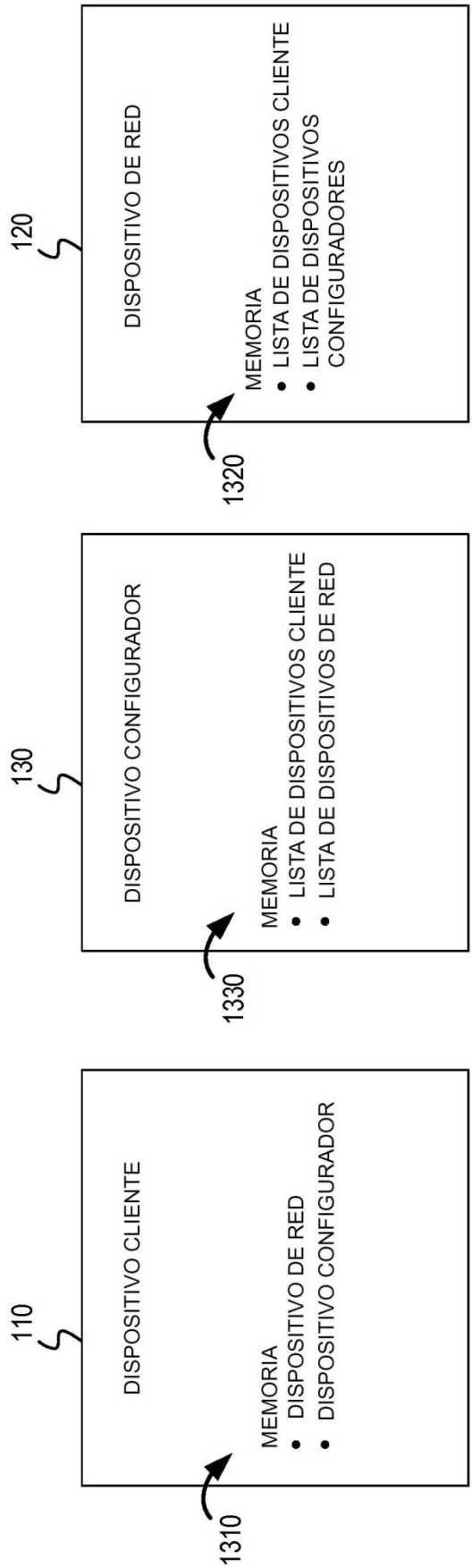
110
DISPOSITIVO CLIENTE
MEMORIA
• DISPOSITIVO DE RED
• DISPOSITIVO CONFIGURADOR
1310
130
DISPOSITIVO CONFIGURADOR
MEMORIA
• LISTA DE DISPOSITIVOS CLIENTE
• LISTA DE DISPOSITIVOS DE RED
1330
120
DISPOSITIVO DE RED
MEMORIA
• LISTA DE DISPOSITIVOS CLIENTE
• LISTA DE DISPOSITIVOS CONFIGURADORES
1320

FIG. 13

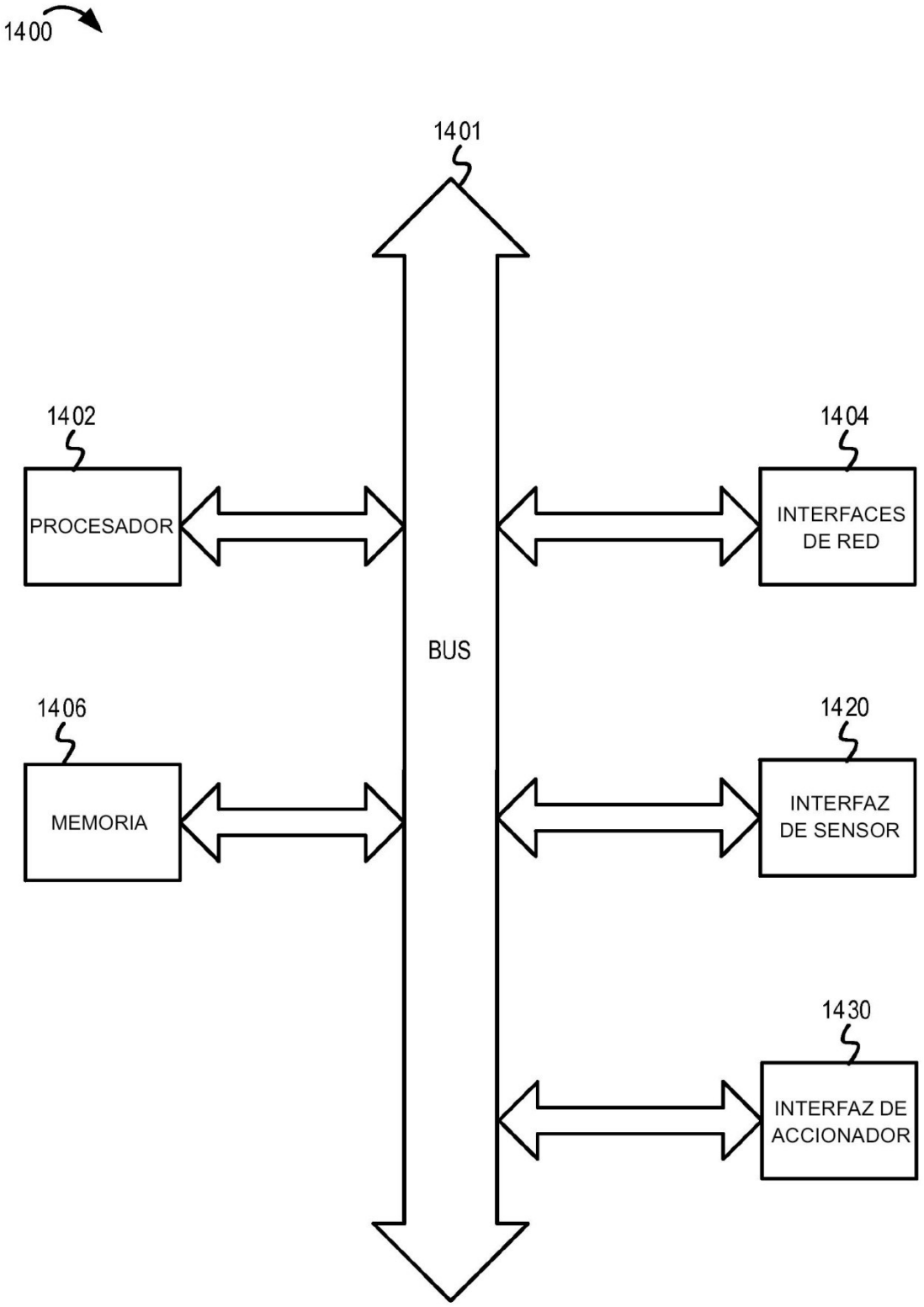
1400
1401
1402
PROCESADOR
1404
INTERFACES DE RED
BUS
1406
MEMORIA
1420
INTERFAZ DE SENSOR
1430
INTERFAZ DE ACCIONADOR

FIG. 14