(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 876 025**

(51) Int. CI.:

G06F 21/32 (2013.01)
H04L 29/06 (2006.01)
H04W 4/00 (2008.01)
H04W 84/18 (2009.01)
H04W 4/80 (2008.01)
H04W 12/00 (2011.01)
H04W 12/06 (2011.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **29.10.2015 PCT/US2015/058150**

(87) Fecha y número de publicación internacional: **12.05.2016 WO16073288**

(96) Fecha de presentación y número de la solicitud europea: **29.10.2015 E 15795269 (8)**

(97) Fecha y número de publicación de la concesión europea: **17.03.2021 EP 3215973**

(54) Título: **Distribuir la autentificación biométrica entre dispositivos en una red *ad hoc***

(30) Prioridad:

04.11.2014 US 201414532608

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
11.11.2021

(73) Titular/es:

QUALCOMM INCORPORATED (100.0%)
5775 Morehouse Drive
San Diego, CA 92121-1714, US

(72) Inventor/es:

JOHN ARCHIBALD, FITZGERALD y
SCHNEIDER, JOHN

(74) Agente/Representante:

FORTEA LAGUNA, Juan José

DESCRIPCIÓN

Distribuir la autentificación biométrica entre dispositivos en una red *ad hoc*

REFERENCIA CRUZADA A SOLICITUD RELACIONADA

[0001] Estas solicitudes reivindican la prioridad y el beneficio de la solicitud no provisional n.º 14/532 608 presentada en la Oficina de Patentes y Marcas de los Estados Unidos el martes, 4 de noviembre de 2014.

ANTECEDENTES

Campo

[0002] Varias características están relacionadas con la autentificación biométrica dentro de redes *ad hoc* inalámbricas, como las redes compuestas por dispositivos informáticos móviles.

Antecedentes

[0003] Una red inalámbrica *ad hoc* es una red inalámbrica descentralizada que no depende de una infraestructura preexistente o de un dispositivo de administración central, como los enrutadores. En lugar de eso, cada nodo de la red participa en el enrutamiento enviando datos a otros nodos. Una red personal inalámbrica *ad hoc* es una red inalámbrica *ad hoc* compuesta por dispositivos personales como teléfonos inteligentes, tabletas, relojes inteligentes, gafas inteligentes, etc. Estas redes pueden tener un dispositivo principal relativamente sofisticado, como un teléfono inteligente o una tableta, junto con varios dispositivos personales secundarios como relojes inteligentes, gafas inteligentes, ropa inteligente, etc., que son relativamente menos sofisticados y capaces que el dispositivo principal.

[0004] Los dispositivos principales, como teléfonos inteligentes o tabletas, pueden estar provistos de sensores biométricos integrados que son relativamente fiables y sofisticados, como sensores de huellas dactilares, para facilitar la autentificación del usuario del dispositivo principal para diversos fines, como compras de consumidores u otras transacciones financieras, acceso seguro al contenido, activación y control seguros, etc. Los sensores biométricos sofisticados típicamente no se proporcionan dentro de dispositivos secundarios como relojes inteligentes, gafas inteligentes o ropa inteligente debido a factores de forma pequeños, consideraciones de coste, consideraciones de longevidad de la batería u otras razones prácticas. No obstante, los dispositivos secundarios pueden requerir autentificación de usuario para diversas aplicaciones, como compras de consumidores. Por ejemplo, puede ser deseable permitir que un usuario realice compras comerciales modestas simplemente moviendo un reloj inteligente sobre un escáner minorista sin requerir que el usuario autorice y autentifique la transacción con un teléfono inteligente más engorroso.

[0005] La FIG. 1 ilustra un ejemplo de una red personal *ad hoc* 100 que tiene un teléfono inteligente 102 como dispositivo principal y un reloj inteligente 104 y un par de gafas inteligentes 106 como dispositivos emparejados secundarios. En este ejemplo, el teléfono inteligente 102 está en comunicación con una red celular a través de una estación base 108 usando señales inalámbricas de acuerdo con una tecnología como evolución a largo plazo (LTE). El teléfono inteligente 102 está en comunicación con el reloj inteligente 104 y las gafas inteligentes 106 a través de un protocolo de transmisión inalámbrica local como Wireless Universal Serial Bus (USB) o Bluetooth™. El teléfono inteligente 102 está equipado para autentificar al usuario del teléfono inteligente usando autentificación biométrica basada en huellas dactilares (usando un sensor de huellas dactilares, no mostrado). El reloj inteligente 104 está equipado para autentificar al usuario usando una autentificación biométrica basada en movimiento menos fiable (como usando un acelerómetro, no mostrado, equipado para detectar un gesto único realizado por el usuario que usa el reloj inteligente). Las gafas inteligentes 106 están equipadas para autentificar al usuario usando autentificación biométrica basada en imágenes faciales (tal como empleando una cámara digital, no mostrada), que también es en general menos fiable que la autentificación de huellas dactilares. La FIG. 1 también ilustra un cajero automático (ATM) 110 que el usuario busca para obtener fondos usando el reloj inteligente 104. Dado que la autentificación basada en movimiento proporcionada por el reloj inteligente no es lo suficientemente fiable, el cajero automático típicamente requeriría que el usuario se autentificara y autorizara la transacción mediante el uso de una tarjeta de débito e introduciendo un código de acceso en un teclado del cajero automático, lo cual puede ser incómodo para el usuario, especialmente si el código de acceso es difícil de recordar y, de hecho, anularía la comodidad de usar el reloj inteligente para activar la transacción. De forma alternativa, el cajero automático podría estar programado para aceptar la autentificación basada en gestos relativamente poco fiable del reloj inteligente, que sería más cómodo para el usuario pero que podría permitir a un ladrón obtener fondos usando un reloj inteligente robado o falsificado simplemente replicando el movimiento de autentificación

[0006] Otra técnica anterior es: PATRICK VERLINDE Y AL: "Multi-modal identity verification using expert fusion", INFORMATION FUSION, vol. 1, n.º 1, julio de 2000 (2000-07), páginas 17-33, XP055242054, ISSN: 1566-2535, DOI: 10.1016/S1566-2535(00)00002-6

[0007] Es necesario proporcionar una autentificación cómoda y fiable para su uso con dispositivos secundarios dentro de una red *ad hoc* de dispositivos principales y secundarios.

BREVE EXPLICACIÓN

[0008] La invención se define en las reivindicaciones adjuntas. Un procedimiento para usar por un dispositivo principal de una red *ad hoc* para la autentificación de un usuario incluye: obtener al menos un parámetro biométrico representativo del usuario del dispositivo principal; determinar un valor de autentificación principal representativo de un grado de autentificación del usuario del dispositivo principal basándose en el al menos un parámetro biométrico; autentificar al usuario del dispositivo principal basándose en el valor de autentificación principal; y compartir el valor de autentificación principal con un dispositivo secundario para facilitar la autentificación del usuario (por ejemplo, mediante el dispositivo secundario). El dispositivo principal y el dispositivo secundario pueden comunicarse a través de una red inalámbrica *ad hoc*.

[0009] En otro aspecto, un dispositivo incluye: un detector de parámetros biométricos configurado para obtener al menos un parámetro biométrico representativo del usuario de un dispositivo principal de una red *ad hoc*; un transmisor; y un circuito de procesamiento configurado para determinar un valor representativo de un grado de autentificación del usuario del dispositivo principal basándose en el al menos un parámetro biométrico, autentificar al usuario del dispositivo principal basándose en el valor representativo del grado de autentificación, y compartir el valor representativo del grado de autentificación con un dispositivo secundario de la red *ad hoc* utilizando el transmisor para facilitar la autentificación del usuario (por ejemplo, mediante el dispositivo secundario).

[0010] En otro aspecto más, un procedimiento para su uso mediante un dispositivo secundario de una red *ad hoc* para la autentificación de un usuario incluye: recibir un valor de autentificación principal representativo de un grado de autentificación de un usuario desde un dispositivo principal de la red *ad hoc*; y determinar si realizar una autentificación secundaria del usuario y, si se va a realizar una autentificación secundaria, (a) obtener al menos un parámetro biométrico utilizando el dispositivo secundario representativo del usuario del dispositivo secundario, (b) determinar un valor de autentificación secundaria representativo de un grado de autentificación del usuario del dispositivo secundario basado en al menos un parámetro biométrico obtenido usando el dispositivo secundario, (c) combinando el valor de autentificación principal recibido del dispositivo principal con el valor de autentificación secundaria para producir un valor de autentificación combinado, y (d) autentificar al usuario del dispositivo secundario utilizando el valor de autentificación combinado.

[0011] En otro aspecto más, un dispositivo incluye: un receptor configurado para recibir un valor de autentificación principal representativo de un grado de autentificación de un usuario desde un dispositivo principal de la red *ad hoc*; un detector de parámetros biométricos; y un circuito de procesamiento configurado para determinar si se debe realizar una autentificación secundaria del usuario y configurado adicionalmente, si se va a realizar una autentificación secundaria, para (a) obtener al menos un parámetro biométrico representativo del usuario de un dispositivo secundario usando el detector de parámetros biométricos, (b) determinar un valor de autentificación secundaria representativo de un grado de autentificación del usuario del dispositivo secundario basado en al menos un parámetro biométrico, (c) combinar el valor de autentificación principal recibido del dispositivo principal con el valor de autentificación secundaria para producir un valor de autentificación combinado, y (d) autentificar al usuario del dispositivo secundario utilizando el valor de autentificación combinado.

BREVE DESCRIPCIÓN DE LOS DIBUJOS

[0012]

La FIG. 1 ilustra una red personal *ad hoc* a modo de ejemplo de dispositivos principales y secundarios con un teléfono inteligente como dispositivo principal.

La FIG. 2 ilustra una red personal *ad hoc* de dispositivos principales y secundarios con autentificación compartida donde un teléfono inteligente es el dispositivo principal.

La FIG. 3 ilustra una red personal *ad hoc* de dispositivos principales y secundarios con autentificación compartida donde un ordenador del vehículo es el dispositivo principal.

La FIG. 4 es un diagrama de tiempos que ilustra las operaciones realizadas por los componentes de una red personal *ad hoc* con un dispositivo principal y secundario, en el que el dispositivo secundario está en comunicación con un dispositivo/sistema al que se accede.

La FIG. 5 es un diagrama de bloques de un sistema en un circuito de procesamiento de chip (SoC) de un dispositivo de comunicación móvil de un dispositivo principal de una red *ad hoc* de acuerdo con un ejemplo

ilustrativo.

La FIG. 6 es un diagrama de bloques de componentes principales y secundarios de una red *ad hoc* de acuerdo con un ejemplo ilustrativo en el que un teléfono inteligente es el dispositivo principal de la red.

La FIG. 7 ilustra un procedimiento a modo de ejemplo para la formación y terminación de una red *ad hoc* usando un teléfono inteligente u otro dispositivo móvil principal.

La FIG. 8 ilustra un procedimiento a modo de ejemplo para la generación de un valor de autentificación principal usando un dispositivo principal de una red *ad hoc*.

La FIG. 9 ilustra un procedimiento a modo de ejemplo para la generación de un valor de autentificación combinado final usando un dispositivo secundario de red *ad hoc*.

La FIG. 10 es un diagrama de bloques de componentes principales y secundarios de una red *ad hoc* de acuerdo con otro ejemplo ilustrativo en el que un controlador de sistemas domésticos es el dispositivo principal de la red.

La FIG. 11 es un diagrama de bloques de componentes principales y secundarios de una red *ad hoc* de acuerdo con otro ejemplo ilustrativo en el que un ordenador de consola de vehículo es el dispositivo principal de la red.

La FIG. 12 ilustra más detalles de un procedimiento a modo de ejemplo para la autentificación de un usuario de una red *ad hoc*.

La FIG. 13 ilustra detalles adicionales de un procedimiento a modo de ejemplo para la desautentificación de un usuario de una red *ad hoc*.

La FIG. 14 es un diagrama de bloques que ilustra un ejemplo de una implementación de hardware para un aparato que emplea un sistema de procesamiento de un dispositivo principal que puede explotar los sistemas, procedimientos y aparatos de las FIGS. 2 - 13.

La FIG. 15 es un diagrama de bloques que ilustra los componentes del circuito de procesamiento del dispositivo principal de la FIG. 14.

La FIG. 16 es un diagrama de bloques que ilustra los componentes de instrucción del medio legible por máquina del dispositivo principal de la FIG. 14.

La FIG. 17 resume un procedimiento a modo de ejemplo para su uso mediante un dispositivo principal de una red *ad hoc* para la autentificación de un usuario.

La FIG. 18 resume aspectos adicionales de un procedimiento a modo de ejemplo para su uso mediante un dispositivo principal de una red *ad hoc* para la autentificación de un usuario.

La FIG. 19 es un diagrama de bloques que ilustra los componentes del circuito de procesamiento de un dispositivo secundario de una red *ad hoc*.

La FIG. 20 es un diagrama de bloques que ilustra los componentes de instrucción del medio legible por máquina del dispositivo secundario de una red *ad hoc*.

La FIG. 21 resume un procedimiento a modo de ejemplo para su uso mediante un dispositivo secundario de una red *ad hoc* para la autentificación de un usuario.

La FIG. 22 resume aspectos adicionales de un procedimiento a modo de ejemplo para su uso mediante un dispositivo secundario de una red *ad hoc* para la autentificación de un usuario.

DESCRIPCIÓN DETALLADA

[0013] En la siguiente descripción, se dan detalles específicos para proporcionar un entendimiento exhaustivo de los diversos aspectos de la divulgación. Sin embargo, un experto en la técnica entenderá que los aspectos se pueden llevar a la práctica sin estos detalles específicos. Por ejemplo, pueden mostrarse circuitos en diagramas de bloques para no complicar los aspectos con detalles innecesarios. En otros casos, pueden no mostrarse con detalle circuitos, estructuras y técnicas que sean muy conocidos para no complicar los aspectos de la divulgación.

[0014] El término "a modo de ejemplo" se usa en el presente documento en el sentido de "que sirve de

ejemplo, caso o ilustración". Cualquier implementación o aspecto descrito en el presente documento como "a modo de ejemplo" no se debe interpretar necesariamente como preferente o ventajoso con respecto a otros aspectos de la divulgación. Asimismo, el término "aspectos" no requiere que todos los aspectos de la divulgación incluyan la característica, ventaja o modo de funcionamiento analizado.

Visión general

[0015] Varias características novedosas pertenecen a la autentificación biométrica dentro de una red personal inalámbrica *ad hoc* o redes similares compuestas por un dispositivo principal y uno o más secundarios. En un ejemplo, se proporciona autentificación biométrica en la que un dispositivo principal (por ejemplo, teléfono inteligente, tableta, etc.) está equipado para realizar autentificación biométrica usando una o más técnicas de autentificación biométrica relativamente sofisticadas y fiables tales como autentificación de huellas dactilares. El dispositivo principal crea una red personal *ad hoc* con uno o más dispositivos secundarios utilizando varias políticas de agrupación, como políticas de proximidad y otros permisos. En un ejemplo, una red inalámbrica *ad hoc* es una red punto a punto entre el dispositivo principal y el dispositivo secundario en la que ninguna otra entidad administra o ayuda en el establecimiento de la conexión punto a punto (por ejemplo, ninguna otra entidad está involucrada en el establecimiento y/o transmisiones a través de la red *ad hoc*). El dispositivo principal comparte un valor de autentificación (por ejemplo, puntuación o nivel de confianza) con otros dispositivos en la red *ad hoc*. Cada dispositivo secundario de la red puede realizar una autentificación de usuario adicional de acuerdo con las preferencias del usuario u otros requisitos. La autentificación secundaria se puede realizar utilizando un sensor de fiabilidad relativamente baja, como una cámara digital (por ejemplo, reconocimiento facial), un micrófono (por ejemplo, reconocimiento de voz) o un acelerómetro (por ejemplo, reconocimiento de gestos). Los resultados de la autentificación secundaria se combinan con el valor de autentificación biométrica (por ejemplo, puntuación o nivel) del dispositivo principal para formar un valor de autentificación final (por ejemplo, puntuación o nivel), que a continuación se utiliza para autentificar al usuario del dispositivo secundario para una o más transacciones como compras de consumidores, acceso seguro al contenido, control seguro, etc. Si no hay requisitos de autentificación de usuario adicionales para un dispositivo secundario en particular, el valor de autentificación biométrica (por ejemplo, puntuación o nivel) del dispositivo principal se mapea al valor de autentificación del dispositivo secundario (por ejemplo, puntuación o nivel).

[0016] La FIG. 2 ilustra un ejemplo de una red personal *ad hoc* 200 que tiene un teléfono inteligente 202 equipado para generar y compartir un valor de autentificación principal (por ejemplo, puntuación o nivel de confianza) y otros datos como reglas de emparejamiento, identificadores de dispositivos (ID), etc. Un reloj inteligente 204 está equipado para recibir el valor de autentificación principal y otros datos y agregar autentificación basada en captura de movimiento al valor de autentificación principal para producir una puntuación de autentificación secundaria combinada final (o nivel de confianza) que es específica para el reloj inteligente 204. Un par de gafas inteligentes 206 también están equipadas para recibir la puntuación de autentificación principal y otros datos. Las gafas inteligentes 206 añaden autentificación basada en imágenes faciales al valor de autentificación principal para producir un valor de autentificación secundaria combinado final (por ejemplo, puntuación o nivel de confianza) que es específico de las gafas inteligentes 206. En este ejemplo, el teléfono inteligente 202 está en comunicación con una red celular a través de una estación base 208 usando señales inalámbricas de acuerdo con cualquier tecnología adecuada pero podría estar en comunicación con sistemas externos usando wifi u otras redes inalámbricas. El teléfono inteligente 202 está en comunicación con el reloj inteligente 204 y las gafas inteligentes 206 a través de cualquier protocolo de transmisión inalámbrica local adecuado. Por ejemplo, el teléfono inteligente puede ser un punto de acceso.

[0017] En el ejemplo de la FIG. 2, el teléfono inteligente 202 está equipado para autentificar inicialmente al usuario con una autentificación biométrica basada en huellas dactilares relativamente fiable (tal como empleando un sensor de huellas dactilares, no mostrado) y para generar el valor de autentificación principal mencionado anteriormente. El valor de autentificación principal puede variar, por ejemplo, dependiendo de la exactitud de la coincidencia entre la huella dactilar de entrada del usuario y una huella dactilar almacenada para el usuario. El teléfono inteligente 202 transmite el valor de autentificación principal resultante a todos los dispositivos secundarios en la red *ad hoc*, asumiendo que los dispositivos secundarios cumplen con los permisos requeridos y los dispositivos están cerca. Para una red *ad hoc* del tipo mostrado en la FIG. 2, el rango de proximidad puede ser bastante pequeño ya que se supone que el usuario llevará o usará todos los dispositivos. El usuario también puede autentificar el reloj inteligente 204, si es necesario, haciendo un movimiento de brazo predeterminado, que es detectado por un acelerómetro interno, que no se muestra por separado. El reloj inteligente 204 genera un valor de autentificación secundaria basado en la exactitud con la cual movimiento del brazo coincide con un patrón de movimiento almacenado para el usuario. El reloj inteligente 204 combina el valor de autentificación secundaria con el valor de autentificación principal recibido del teléfono inteligente 202 para generar y guardar un valor de autentificación combinado final. Este valor puede compararse posteriormente con varios umbrales predeterminados para autentificar transacciones particulares. Tenga en cuenta que si el reloj inteligente requiere autentificación de usuario por separado puede depender de varios factores, como el valor de autentificación principal. Si el valor de autentificación principal es relativamente alto y, por lo tanto, fiable, es posible que no se requiera la autentificación secundaria. Si la autentificación principal es más baja y, por lo tanto, menos fiable, es posible que se requiera una autentificación secundaria. Como otro

ejemplo, es posible que se requiera autentificación secundaria si el reloj inteligente está habilitado para realizar transacciones financieras, pero no se requiera si solo está habilitado para realizar otras transacciones.

[0018] De manera similar, se puede requerir que el usuario se autentifique ante las gafas inteligentes 206 haciendo que las gafas tomen una foto digital del rostro del usuario. A continuación, las gafas inteligentes generan un valor de autentificación secundaria basado en la exactitud con la cual la foto coincide con una imagen prealmacenada del usuario y combina el valor de autentificación secundaria con el valor de autentificación principal recibido del teléfono inteligente para generar y guardar un valor de autentificación combinado final. La autentificación inicial del usuario a través de los dispositivos principal y secundario de la red puede requerirse con relativa poca frecuencia para no molestar al usuario. Siempre que un dispositivo secundario deje de estar cerca del teléfono inteligente (o no cumpla con otros permisos o parámetros requeridos), el dispositivo se desautentifica y no se puede usar para autorizar transacciones o acceder a sistemas/dispositivos a menos que se vuelva a autentificar.

[0019] En algún momento, el usuario puede buscar obtener dinero en efectivo de un cajero automático 210 moviendo el reloj inteligente cerca de un escáner de campo cercano (no mostrado por separado) del cajero automático. El reloj inteligente 204 detecta el intento de obtener efectivo basándose en las señales de respuesta recibidas del cajero automático y verifica que el valor de autentificación final sea suficiente para autorizar la transacción, por ejemplo, comparando el valor de autentificación final del reloj inteligente con un umbral predeterminado para el retiro de efectivo. . El umbral puede variar dependiendo de la cantidad de efectivo a retirar, de modo que se requiera un mayor grado de autentificación para cantidades mayores. Si el valor de autentificación final para el reloj inteligente 204 excede el umbral apropiado, el usuario del reloj inteligente 204 está debidamente autentificado para la transacción. El reloj inteligente a continuación transmite cualquier credencial requerida al cajero automático (como el código de acceso o el número de identificación personal (PIN) asociado con la cuenta del cajero automático) para completar la transacción. Suponiendo que las credenciales sean satisfactorias, el cajero automático suministra el efectivo.

[0020] De esta manera, el usuario puede realizar cómodamente transacciones financieras modestas sin la carga de requerir autentificación simultánea usando el teléfono inteligente (que puede guardarse en el bolso o maletín del usuario o guardarse en un bolsillo con cremallera o abotonado) y sin necesidad de introducir ningún PIN o contraseña directamente en el cajero automático (lo cual podría ser incómodo para el usuario si la contraseña es difícil de recordar y anularía la comodidad de usar el reloj inteligente para activar la transacción). Sin embargo, estas transacciones son sustancialmente seguras porque se emplean dos tipos de autentificación: la autentificación inicial basada en huellas dactilares del teléfono inteligente y la autentificación basada en captura de movimiento del reloj inteligente. Además, el reloj inteligente debe estar muy cerca del teléfono inteligente durante la transacción; de lo contrario, el reloj inteligente no se autentificará y no podrá autorizar la transacción.

[0021] Tenga en cuenta también que ninguno de los procedimientos de autentificación individuales necesita ser perfecto siempre que el valor final combinado sea suficientemente alto. Por ejemplo, la autentificación de huellas dactilares inicial puede no ser perfecta debido a una huella dactilar ligeramente manchada. Del mismo modo, el usuario no necesita emular exactamente el movimiento del brazo requerido al autentificar el reloj inteligente. Sin embargo, el valor de autentificación combinado puede, no obstante, ser suficientemente alto para autentificar de manera fiable al usuario para transacciones particulares. En otros ejemplos, el reloj inteligente no requiere autentificación secundaria y el valor de autentificación principal simplemente se mapea al reloj inteligente. Como se señaló, el umbral para la autentificación puede depender del tipo y cantidad de la transacción, y se requiere una autentificación biométrica más precisa para transacciones financieras más grandes. Tenga en cuenta también que si se considera que el usuario no está lo suficientemente autentificado para la transacción basándose en el valor combinado final del reloj inteligente 204, el usuario aún puede autentificar directamente la transacción introduciendo el PIN en el teclado del cajero automático o usando el teléfono inteligente volviendo a aplicar la huella digital al sensor biométrico del teléfono inteligente.

[0022] Como otro ejemplo de transacción para usar con la red *ad hoc* de la FIG. 2, el usuario puede desear acceder a información confidencial desde un sitio web de Internet a través de las gafas inteligentes 206. Las gafas inteligentes 206 compararán su valor de autentificación final con un umbral predeterminado para determinar si el usuario de las gafas inteligentes está suficientemente autentificado para permitir el acceso al sitio web en particular. Si el valor de autentificación final supera el umbral, el usuario se autentifica y las credenciales de acceso adecuadas (por ejemplo, contraseñas o PIN) se envían al sitio web a través de Internet para obtener acceso al sitio web. La información solicitada se descarga a través de Internet y se muestra a través de las gafas inteligentes. De esta manera, el usuario puede acceder cómodamente a información confidencial a través de las gafas inteligentes sin la carga de requerir la entrada directa de contraseñas o PIN. Sin embargo, existe poco o ningún riesgo de que una persona no autorizada pueda acceder a la información utilizando las gafas inteligentes extraviadas o robadas de otra persona, ya que las gafas se anularían la autentificación una vez que ya no estén más cerca del teléfono inteligente del usuario.

[0023] La FIG. 3 ilustra otro ejemplo de una red 300 personal *ad hoc*. En el ejemplo, el ordenador de la

consola del salpicadero de un coche 302 u otro vehículo es el dispositivo principal de la red *ad hoc*. Los distintos dispositivos móviles de los ocupantes del vehículo son los dispositivos secundarios. En el ejemplo de la FIG. 3, los dispositivos secundarios a modo de ejemplo incluyen un teléfono inteligente 304, un par de gafas inteligentes 306 y una tableta 308. El ordenador de la consola del tablero de instrumentos del automóvil 302 se muestra en comunicación con una red celular a través de una o más estaciones base 310. En el ejemplo de la FIG. 3, la consola del tablero incluye un sensor de huellas dactilares (u otro sensor biométrico adecuado, que no se muestra por separado) que autentifica al operador del vehículo para permitir el funcionamiento del vehículo y también para permitir el acceso de varios dispositivos móviles secundarios a una red inalámbrica dentro del vehículo como un punto caliente de vehículo. La consola del tablero de instrumentos del automóvil 302 genera el valor de autentificación principal mencionado anteriormente para la transmisión a todos los dispositivos secundarios en la red *ad hoc* del vehículo, asumiendo que los dispositivos secundarios cumplen con los permisos requeridos y permanecen en la proximidad. En un caso típico, los diversos dispositivos de los miembros de la familia están prerregistrados en el automóvil y, por lo tanto, se les otorga automáticamente acceso al punto de acceso dentro del automóvil. Para la red de la FIG. 3, el rango de proximidad será más amplio que el de la FIG. 2 ya que algunos pasajeros pueden estar en el asiento delantero mientras que otros están en el asiento trasero. Además, la proximidad puede establecerse de manera que los dispositivos permanezcan en la red *ad hoc* siempre que los dispositivos estén relativamente cerca del vehículo, lo cual permite a los ocupantes llevar sus dispositivos desde el vehículo en las paradas de descanso o similares sin ser desconectados inmediatamente de la red *ad hoc*. Una vez que se lleva un dispositivo lo suficientemente lejos del vehículo, se desautentifica el dispositivo. En otros ejemplos, una vez que se quita un dispositivo del automóvil, se desautentifica inmediatamente y se quita de la red *ad hoc*.

[0024] Si bien la red *ad hoc* es válida (por ejemplo, mientras los ocupantes permanecen sentados dentro del vehículo), los ocupantes individuales pueden, por ejemplo, descargar contenido multimedia de la memoria de los componentes del vehículo (con sujeción a cualquier bloqueo de contenido impuesto por el propietario del vehículo). Como ejemplo, los niños pasajeros pueden acceder cada uno a diferentes medios almacenados (como música, películas, programas de televisión, etc.) desde el vehículo a través de sus propios dispositivos personales utilizando la red *ad hoc*. De lo contrario, el acceso a dicho contenido multimedia podría requerir una autentificación onerosa de cada dispositivo individual. Con la autentificación compartida a través de la red *ad hoc* del vehículo, cada dispositivo individual se autentifica automática y cómodamente basándose en el valor de autentificación del operador del vehículo. El ordenador de la consola del automóvil puede programarse para permitir que diferentes operadores del vehículo autoricen contenido multimedia diferente (o no). Por ejemplo, cuando un conductor adolescente está haciendo funcionar el vehículo, se puede permitir una autentificación de dispositivo secundaria mínima o nula para limitar la distracción general del conductor.

[0025] Otros ejemplos de redes *ad hoc* vehiculares incluyen redes dentro de otros tipos de vehículos como autobuses, camiones, aviones, embarcaciones, motocicletas, etc. Otras redes *ad hoc* pueden incluir dispositivos de supervisión de salud, como monitores de frecuencia cardíaca o monitores de presión arterial que pueden emparejarse con un teléfono inteligente o una tableta. Dichos dispositivos de control de la salud se pueden autorizar selectivamente para compartir información con un sistema de control de la salud remoto, como un sistema operado por un médico u otro proveedor de atención médica. Otras redes *ad hoc* pueden incluir redes de control de edificios que controlan las operaciones de los electrodomésticos dentro de una casa u otra estructura, como mediante el control de termostatos, monitores de seguridad, persianas, etc. En un ejemplo, la detección de una intrusión en una casa por un extraño desencadena una desautentificación inmediata de todos los dispositivos dentro de la red *ad hoc* doméstica, al menos para fines seleccionados. Los ejemplos de algunos de estos sistemas *ad hoc* se describen con mayor detalle a continuación.

[0026] La FIG. 4 resume algunas de las características de las redes *ad hoc* mencionadas anteriormente con referencia a un diagrama de tiempo 400 que ilustra las operaciones de un dispositivo principal 402, un dispositivo secundario 404 y un dispositivo o sistema 406 al que se debe acceder (como un cajero automático, un sitio web seguro, etc. .) En 408, el dispositivo principal introduce parámetros principales de autentificación biométrica tales como escaneos de huellas dactilares y, en 410, genera un valor de autentificación principal basado en los parámetros principales de autentificación biométrica y comparte el valor con el dispositivo secundario 404. En 412, el dispositivo secundario 404 introduce parámetros de autentificación biométrica secundarios tales como captura de movimiento o parámetros de reconocimiento facial (asumiendo que la autentificación secundaria está habilitada). En 414, el dispositivo secundario 404 genera un valor de autentificación secundaria y lo combina con el valor de autentificación principal para formar un valor de autentificación final para el dispositivo secundario. El sistema/dispositivo 406 detecta un intento de acceso por parte del usuario 415, tal como un intento de obtener efectivo desde un cajero automático, acceder a un sitio web, etc. En respuesta, en 416, el dispositivo secundario 404 intenta autentificar al usuario para el acceso solicitado basándose en el valor de autentificación final. Como ya se señaló, la autentificación puede depender del sistema o dispositivo particular al que se va a acceder y del propósito del acceso con un valor de autentificación más alto requerido para acceder a sistemas más sensibles o para iniciar transacciones financieras de mayor valor. Si está autentificado, el dispositivo secundario 404 envía a continuación las credenciales apropiadas (como contraseñas o PIN) al sistema/dispositivo 406 para acceder 418. El sistema/dispositivo 406 verifica las credenciales 420 y proporciona los datos a los que se accede al dispositivo

secundario (si se verifican las credenciales) o envía una confirmación de transacción 422 en el caso de una transacción financiera completada o similar. El dispositivo secundario 404 reenvía una confirmación de acceso o una notificación de denegación 424 al dispositivo principal 402, dependiendo de si el usuario fue debidamente autentificado y las credenciales fueron aceptadas.

[0027] Aunque no se muestra en la FIG. 4, el dispositivo secundario puede desautentificarse tras la detección de varios factores desencadenantes, como la retirada del dispositivo secundario de la proximidad del dispositivo principal. Al detectar eventos de desautentificación utilizando el dispositivo principal de la red, los dispositivos secundarios en la red *ad hoc* también se desautentificaron. Al detectar eventos de desautentificación en un dispositivo secundario, todos los demás dispositivos secundarios en la red ad-hoc también se desautentificaron. Al detectar una "condición de amenaza" por parte de un dispositivo secundario, se emite una petición de desautentificación al dispositivo principal, además de la desautentificación del dispositivo secundario. Los ejemplos de condiciones de amenaza incluyen la violación de reglas de red *ad hoc* (por ejemplo, reglas de proximidad) detectadas por un dispositivo secundario que indica un compromiso en el dispositivo principal. Otros ejemplos incluyen cualquier indicación de que un dispositivo podría ser falsificado, pirateado o comprometido de otra manera.

[0028] Entre las características de las redes *ad hoc* descritas en el presente documento: una experiencia de usuario potencialmente mejor en dispositivos secundarios; eliminación de la autentificación redundante; creación perfecta de redes de seguridad *ad hoc*; y seguridad mejorada en el dispositivo principal. Para resumir, la autentificación biométrica en al menos algunas de las redes personales *ad hoc* descritas en el presente documento incluye: formar una red personal *ad hoc* usando las preferencias del usuario (por ejemplo, definición de proximidad, permisos del dispositivo); compartir un valor de autentificación biométrica (por ejemplo, puntuación o nivel) desde un dispositivo principal a los dispositivos secundarios en la red ad-hoc; combinar un valor biométrico compartido con una autentificación secundaria de baja fiabilidad en dispositivos secundarios para formar un valor de autentificación final; y mapeo del valor biométrico a la autentificación del dispositivo secundario. La red *ad hoc* también puede proporcionar: la desautentificación de un dispositivo secundario después de la desautentificación en el dispositivo principal; desautentificación de dispositivos secundarios en caso de violación de las reglas de la red; y emitir de forma remota la desautentificación al dispositivo principal tras la detección de amenazas en los dispositivos secundarios.

Sistemas, procedimientos y componentes de red *ad hoc* a modo de ejemplo

[0029] Se describirán ahora varios sistemas y procedimientos a modo de ejemplo para su uso con redes *ad hoc* personales. En muchos de los ejemplos, se utiliza un teléfono inteligente como dispositivo principal. En aras de la exhaustividad, se expondrá una breve descripción del hardware de un teléfono inteligente a modo de ejemplo, que incluye componentes para generar y compartir valores de autentificación principal. Otros dispositivos principales como tabletas, consolas de automóvil o similares pueden incluir al menos algunos componentes similares.

[0030] La FIG. 5 ilustra un sistema en un circuito de procesamiento de chip (SoC) 500 de un teléfono inteligente u otro dispositivo de comunicación móvil de acuerdo con un ejemplo en el que se pueden explotar varias características novedosas. El circuito de procesamiento de SoC puede ser un circuito de procesamiento Snapdragon™ fabricado por Qualcomm Incorporated. El circuito de procesamiento de SoC 500 incluye un circuito de procesamiento de aplicaciones 510, que incluye una CPU de múltiples núcleos 512. El circuito de procesamiento de aplicaciones 510 típicamente controla el funcionamiento de todos los componentes del dispositivo de comunicación móvil. En un aspecto, el circuito de procesamiento de aplicaciones 510 incluye un controlador de autentificación biométrico principal 513 equipado para generar un valor de autentificación principal (por ejemplo, puntuación o nivel), que a continuación se comparte con otros dispositivos dentro de la red *ad hoc* de la cual el teléfono inteligente es el dispositivo principal. . El circuito de procesamiento de aplicaciones 510 también incluye un controlador de red *ad hoc* 515 para controlar la formación y terminación de una red *ad hoc* con varios dispositivos secundarios. El circuito de procesamiento de aplicaciones 510 puede incluir una ROM de arranque 518 que almacena instrucciones de secuencia de arranque para los diversos componentes del circuito de procesamiento de SoC 500. El circuito de procesamiento de SoC 500 incluye además uno o más subsistemas periféricos 520 controlados por el circuito de procesamiento de aplicaciones 510. Los subsistemas periféricos 520 pueden incluir, entre otros, un subsistema de almacenamiento (por ejemplo, memoria de solo lectura (ROM), memoria de acceso aleatorio (RAM)), un subsistema de vídeo/gráficos (por ejemplo, circuito de procesamiento de señales digitales (DSP), procesamiento de gráficos unidad de circuito (GPU)), un subsistema de audio (por ejemplo, DSP, convertidor de analógico a digital (ADC), convertidor de digital a analógico (DAC)), un subsistema de administración de energía, subsistema de seguridad (por ejemplo, cifrado, derechos digitales (DRM)), un subsistema de entrada/salida (E/S) (por ejemplo., teclado, pantalla táctil) y subsistemas de conectividad cableada e inalámbrica (por ejemplo., bus serie universal (USB), sistema de posicionamiento global (GPS), wifi, sistema global Móvil (GSM), acceso múltiple por división de código (CDMA), módems 4G evolución a largo plazo (LTE)). El subsistema periférico 520 a modo de ejemplo, que es un subsistema de módem, incluye un DSP 522, varios componentes 524 de hardware (HW) y software (SW), y varios componentes 526 de radiofrecuencia (RF). En un aspecto, cada subsistema

periférico 520 también incluye una ROM de arranque 528 que almacena una imagen de arranque principal (no mostrada) de los subsistemas periféricos 520 asociados.

[0031] El circuito de procesamiento SoC 500 incluye además varios recursos HW internos compartidos 530, como un almacenamiento interno compartido 532 (por ejemplo, RAM estática (SRAM), RAM dinámica síncrona (SD) de velocidad de datos doble (DDR), DRAM, memoria Flash, etc.), que es compartido por el circuito de procesamiento de aplicaciones 510 y varios subsistemas periféricos 520 para almacenar varios datos de tiempo de ejecución. En un aspecto, los componentes 510, 518, 520, 528 y 530 del circuito de procesamiento SoC 500 pueden integrarse en un sustrato de un solo chip. El circuito 500 de procesamiento de SoC incluye además varios recursos 540 de HW compartidos externos, que pueden estar ubicados en un sustrato de chip diferente y comunicarse con el circuito 500 de procesamiento de SoC a través de un bus del sistema (no mostrado). Los recursos HW compartidos externos 540 pueden incluir, por ejemplo, un almacenamiento compartido externo 542 (por ejemplo, DDR RAM, DRAM, memoria Flash) y/o almacenamiento permanente de datos 544 (por ejemplo, una tarjeta Secure Digital (SD) o una unidad de disco duro (HDD), etc.), que son compartidos por el circuito de procesamiento de aplicaciones 510 y varios subsistemas periféricos 520 para almacenar varios tipos de datos, como información de un sistema operativo (SO), archivos del sistema, programas, aplicaciones, datos de usuario, archivos de audio/vídeo, etc. Cuando se activa el dispositivo de comunicación móvil que incorpora el SoC, el circuito de procesamiento de SoC seguro 500 comienza un proceso de arranque del sistema. En particular, el circuito de procesamiento de aplicaciones 510 accede a la ROM de arranque 518 para recuperar instrucciones de arranque para el circuito de procesamiento de SoC 500, incluyendo instrucciones de secuencia de arranque para varios subsistemas periféricos 520. Los subsistemas periféricos 520 también pueden tener una RAM de arranque periférica adicional 528. Además, el teléfono inteligente incluye un dispositivo de entrada biométrica 550 tal como un escáner de huellas dactilares o un escáner de iris para introducir parámetros biométricos de un usuario para generar el valor de autentificación biométrico principal mediante el controlador de autentificación biométrica 513. Dependiendo de la implementación, el escáner de iris puede aprovechar una cámara digital (no se muestra por separado) del teléfono inteligente.

[0032] La FIG. 6 ilustra componentes seleccionados de dispositivos dentro de una red *ad hoc* móvil a modo de ejemplo 600 donde el dispositivo principal es un teléfono inteligente 602 y los dispositivos secundarios incluyen un reloj inteligente 604, gafas inteligentes 606 y un monitor de salud 607 tal como un monitor de frecuencia cardíaca o similar. Solo los componentes internos seleccionados pertinentes a la red *ad hoc* se muestran dentro de los distintos dispositivos. Cada dispositivo incluirá otros componentes para implementar las otras funciones del dispositivo. Haciendo referencia primero al teléfono inteligente 602, un controlador de red *ad hoc* 608 controla la formación y terminación de una red *ad hoc* usando un controlador de evaluación de elementos comunes 610 y un controlador de evaluación de permisos 612. El controlador de evaluación de elementos comunes detecta cualquier dispositivo secundario en comunicación con el teléfono inteligente 602 a través de un controlador de comunicación 614 (que tiene una antena 615) y evalúa el grado de elementos comunes entre el teléfono inteligente y el dispositivo secundario. En un ejemplo típico, el controlador de comunicación 614 puede ser un controlador de punto de acceso pero puede corresponder a cualquier dispositivo adecuado para comunicarse directamente (o mediante sistemas intermedios) con los dispositivos secundarios. Además, típicamente, los diversos dispositivos secundarios del usuario están prerregistrados para su uso con el teléfono inteligente 602 de modo que el teléfono inteligente puede ignorar todos y cada uno de los dispositivos secundarios que no están prerregistrados.

[0033] Suponiendo que un dispositivo secundario en particular está en comunicación con el teléfono inteligente y está prerregistrado, como el reloj inteligente 604, el controlador de evaluación de elementos comunes 610 detecta u obtiene de otro modo varios parámetros asociados con el teléfono inteligente y el dispositivo secundario a partir de los cuales puede detectarse, medirse, determinarse o evaluarse de otro modo un grado de elementos comunes de los dos dispositivos. Si se encuentra un grado suficiente de elementos comunes, se invita al dispositivo secundario a la red *ad hoc* del dispositivo principal. Por ejemplo, el controlador de evaluación de elementos comunes 610 del teléfono inteligente puede detectar la ubicación del teléfono inteligente y el reloj inteligente 604 basándose en señales de GPS y determinar que los dos dispositivos tienen suficientes elementos comunes si están muy próximos entre sí. El grado de proximidad requerido puede estar preprogramado y, como se indicó anteriormente, puede ser relativamente exacto para una red *ad hoc* personal compuesta por dispositivos de usuario destinados a ser transportados o usados por un usuario. En algunos casos, el mero hecho de que un dispositivo secundario esté en comunicación con el dispositivo principal es suficiente para establecer el grado de proximidad requerido, especialmente si la comunicación se logra a través de una comunicación de rango relativamente corto, como un punto de acceso wifi.

[0034] De forma adicional o alternativa, el controlador de evaluación de elementos comunes 610 puede evaluar parámetros tales como movimiento, ruido ambiental, luz ambiental, etc., para evaluar elementos comunes. Por ejemplo, el teléfono inteligente 602 puede usar su micrófono o cámara para supervisar el ruido ambiental y las condiciones de luz ambiental para comparar con el ruido ambiental y las condiciones de luz detectadas a través del micrófono o la cámara de un dispositivo secundario (como las gafas inteligentes 606). Si se encuentra que los dispositivos detectan la misma luz ambiental o ruido, se considera que están en el mismo lugar. A continuación, el controlador de evaluación de elementos comunes 610 combina los diversos

parámetros representativos de elementos comunes en un único valor de comparación con un umbral de elementos comunes para determinar si un dispositivo secundario particular debe ser invitado a la red *ad hoc*. En algunos ejemplos, los elementos comunes se especifican mediante un conjunto de reglas de elementos comunes que, si se violan, desencadenan la desautentificación de un dispositivo secundario en particular o, en algunos casos, la terminación de toda la red *ad hoc*. Suponiendo que se va a invitar a un dispositivo secundario particular, como el reloj inteligente 604, a la red *ad hoc*, se pueden generar y transmitir señales de emparejamiento adecuadas a través del controlador de comunicación 614.

[0035] En lo que respecta a los permisos, el controlador de evaluación de permisos 612 puede estar preprogramado con varias reglas de permisos de red *ad hoc* aplicables a varios dispositivos secundarios. Estos permisos pueden incluir la condición de registro antes mencionada por la cual solo los dispositivos secundarios que se hayan prerregistrado con el dispositivo principal se pueden permitir en la red *ad hoc*. Sin embargo, otros permisos pueden especificar que un dispositivo registrado en particular solo se puede agregar a la red *ad hoc* bajo ciertas condiciones. Por ejemplo, se pueden agregar ciertos dispositivos a la red *ad hoc* dependiendo de la red de comunicación que se esté usando, agregando un dispositivo particular si se usa Bluetooth™ pero no si se usa wifi, o viceversa. Si el usuario aún no ha sido autentificado en el teléfono inteligente 602, se puede usar un escáner de huellas dactilares o iris 616 para introducir características biométricas, que a continuación se autentifican mediante un controlador de autentificación de iris y/o huellas dactilares 618. El valor de autentificación principal mencionado anteriormente (y otros datos tales como las ID de dispositivo para los diversos dispositivos dentro de la red *ad hoc*) pueden enviarse a continuación a los diversos dispositivos secundarios.

[0036] El reloj inteligente 604 se muestra con un controlador de comunicación 620 y una antena 621 para recibir señales del teléfono inteligente 602 (ya sea directamente o mediante una red de comunicación intermedia). El reloj inteligente también incluye un controlador de emparejamiento 622 que responde a cualquier señal de emparejamiento recibida desde el teléfono inteligente 602 y envía señales de protocolo de enlace de respuesta para unirse a la red *ad hoc*. En algunos casos, el dispositivo secundario iniciará el acceso a la red *ad hoc* detectando el dispositivo principal y enviando una señal solicitando unirse a la red *ad hoc*. Esto puede ayudar a reducir el consumo de energía en el dispositivo principal al eliminar la necesidad de que el dispositivo principal supervise periódica o continuamente la presencia del dispositivo secundario. En un ejemplo, cada vez que se activa el reloj inteligente 604, envía una señal que anuncia su presencia, a la que el teléfono inteligente puede responder, si también está activo en un rango de comunicación. Si se requiere autentificación secundaria con el reloj inteligente 604 (según se determine basándose, por ejemplo, en permisos o reglas recibidas del teléfono inteligente), dicha autorización secundaria se puede realizar usando un acelerómetro 624 para detectar un movimiento de usuario distintivo y preprogramado y un controlador de autorización de reconocimiento de movimiento 626 y que realiza la autentificación secundaria.

[0037] Las gafas inteligentes 606 incluyen componentes similares. En resumen, las gafas inteligentes tienen un controlador de comunicación 628, una antena 630 y un controlador de emparejamiento 632 (así como muchos otros componentes para implementar las funciones de las gafas inteligentes, no mostrados). Si se requiere autentificación secundaria, la autorización secundaria puede realizarse usando una cámara 634 para detectar una imagen facial y un controlador de autorización de reconocimiento facial 636 y que realiza la autentificación secundaria. El monitor de salud 607 también tiene un controlador de comunicación 640, una antena 641 y un controlador de emparejamiento 638 (así como otros componentes para implementar las funciones del monitor de salud, no mostradas). En este ejemplo, el monitor de salud no tiene capacidad de autentificación secundaria y, por lo tanto, simplemente usa el valor de autentificación principal recibido del teléfono inteligente 602. Aunque la FIG. 6 solo muestra un reloj inteligente a modo de ejemplo, un par de gafas inteligentes y un monitor de salud, dispositivos secundarios adicionales o alternativos pueden formar la red *ad hoc*, incluyendo ropa inteligente, dispositivos de juego y otros dispositivos móviles de función completa como tabletas u otros teléfonos inteligentes.

[0038] La FIG. 7 es un diagrama de flujo 700 que ilustra la formación y terminación de una red *ad hoc* usando un teléfono inteligente u otro dispositivo principal. El dispositivo principal detecta uno o más dispositivos secundarios en comunicación con el dispositivo principal que están autorizados para emparejarse con el dispositivo principal en una red *ad hoc* y detecta elementos comunes basados en la proximidad, el entorno ambiental compartido (sonido, luz, movimiento, etc.) o compartido red de comunicación 702. El dispositivo principal evalúa el grado de elementos comunes de los dispositivos principales y secundarios y determina cualquier permiso explícito requerido para los dispositivos secundarios 704. Para cada dispositivo secundario que tenga suficientes elementos comunes con el dispositivo principal según se determine basándose en las reglas de elementos comunes y que coincida con todos los permisos necesarios, el dispositivo principal envía una señal de emparejamiento para invitar al dispositivo secundario a la red *ad hoc* o recibir la señal de emparejamiento del dispositivo secundario 706. El dispositivo principal recibe señales de respuesta de los dispositivos secundarios y forma la red *ad hoc* compuesta por el dispositivo principal y todos los dispositivos secundarios que aceptaron las señales de invitación de emparejamiento y permanecen en la proximidad 708.

[0039] El dispositivo principal comparte información a pedido, o según sea necesario, con los diversos

dispositivos secundarios de la red *ad hoc*, tales como valores de autentificación, compartir ID, permisos, reglas comunes, etc. 710. El dispositivo principal supervisa las condiciones de desautentificación del dispositivo secundario, como la desautentificación manual del usuario, la falta de comunicación, las violaciones de las reglas comunes y/o fallos en los permisos, y responde desactivando todos y cada uno de los dispositivos secundarios que requieren desautentificación 712. El dispositivo principal supervisa las condiciones de desautentificación del dispositivo principal, como la desautentificación manual del usuario y/o las condiciones de amenaza (incluida la sospecha de suplantación de identidad o piratería) y responde eliminando la autentificación del dispositivo principal y todos los dispositivos secundarios y termina la red *ad hoc* 714. En lo que respecta a la aceleración repentina, el dispositivo puede detectar la aceleración repentina asociada con la caída del dispositivo y enviar señales de desautentificación a los dispositivos secundarios para terminar la red *ad hoc* con la expectativa de que el dispositivo principal se dañará y, a partir de entonces, podría no ser capaz de realizar desautentificación de los dispositivos secundarios.

[0040] La FIG. 8 es un diagrama de flujo 800 que ilustra la generación de un valor de autentificación principal usando un teléfono inteligente u otro dispositivo principal. El dispositivo principal inicia la autentificación principal al inicio del dispositivo o al detectar otros desencadenantes de autentificación, como una desautentificación previa 802. El dispositivo principal introduce parámetros principales de autentificación biométrica usando un dispositivo de entrada biométrica como un escáner de huellas dactilares o un escáner de iris 804. El dispositivo principal extrae características biométricas de los parámetros de entrada, como minucias de huellas dactilares y/o anillos y surcos del iris, y las compara con características prealmacenadas para calcular un valor de autentificación principal representativo de un grado en el que las características biométricas coinciden con las características prealmacenadas correspondientes de un usuario autorizado del dispositivo 806. El dispositivo principal almacena el valor de autentificación principal dentro del dispositivo y lo transmite a cualquier dispositivo secundario actualmente en una red *ad hoc* existente para su uso en la autorización de cualquier transacción solicitada por un usuario del dispositivo secundario 808. El dispositivo principal emplea el valor de autentificación principal para autentificar cualquier transacción solicitada por el usuario mediante el uso del dispositivo principal, como transacciones financieras, acceso seguro al contenido, control seguro, etc. 810. El dispositivo principal detecta y responde a cualquier condición de desautentificación del dispositivo principal, como los activadores de desautentificación principal enviados desde uno de los dispositivos secundarios de la red *ad hoc* 812.

[0041] La FIG. 9 es un diagrama de flujo 900 que ilustra la generación de un valor de autentificación combinado final utilizando un dispositivo secundario de una red *ad hoc*. El dispositivo secundario inicia la autentificación del dispositivo secundario al iniciarse el dispositivo o al detectar otros desencadenantes de autentificación, como una desautentificación anterior 902. El dispositivo secundario recibe el valor de autentificación del dispositivo principal del dispositivo principal de la red *ad hoc* y determina si se requiere autentificación secundaria 904. Si se requiere autentificación secundaria, el dispositivo secundario introduce parámetros de autentificación biométrica secundarios usando un dispositivo de entrada biométrica como un acelerómetro para reconocimiento de movimiento, una cámara digital para reconocimiento facial o un micrófono para reconocimiento de voz 906. Si se requiere autentificación secundaria, el dispositivo secundario extrae características biométricas de los parámetros de entrada, como datos de captura de movimiento, características faciales o indicios de patrones de voz y las compara con características almacenadas previamente para calcular un valor de autentificación secundaria representativo de un grado en el que las características biométricas coinciden con las características prealmacenadas correspondientes de un usuario del dispositivo 908.

[0042] Si se requiere autentificación secundaria, el dispositivo secundario combina el valor de autentificación secundaria con el valor de autentificación principal recibido del dispositivo principal para producir un valor de autentificación final combinado o de lo contrario mapea la autentificación principal al valor de autentificación final combinado sin autentificación secundaria 910. El dispositivo secundario emplea el valor de autentificación combinado final para autentificar cualquier transacción solicitada por el usuario a través del dispositivo secundario, como transacciones financieras, acceso seguro al contenido, control seguro, etc. 912. El dispositivo secundario detecta y responde a cualquier condición de desautentificación del dispositivo principal o secundario, incluida la generación de un activador de desautentificación del dispositivo principal para enviarlo al dispositivo principal en caso de una condición de amenaza grave 914, como una indicación de que el dispositivo principal ha sido objeto de una suplantación de identidad o piratería. Tenga en cuenta que, en algunos casos, el dispositivo secundario de una red *ad hoc* en particular puede ser un dispositivo con todas las funciones, como una tableta o un teléfono inteligente, que tiene las mismas o mayores capacidades que el dispositivo principal de la red. Como tal, el dispositivo secundario puede tener la capacidad de detectar una condición de amenaza que el dispositivo principal no detecta. Al menos por esta razón, es útil permitir que un dispositivo secundario de la red envíe un activador de desautentificación al dispositivo principal y a todos los demás dispositivos de la red.

[0043] La FIG. 10 ilustra componentes seleccionados de dispositivos dentro de una red 1000 *ad hoc* basada en el hogar a modo de ejemplo donde el dispositivo principal es un controlador 1002 de sistemas domésticos y los dispositivos secundarios incluyen una tableta del propietario 1004 y una tableta del invitado 1006. Solo los componentes internos pertinentes a la red *ad hoc* se muestran dentro de los distintos dispositivos. Algunos de

los componentes son iguales o similares a los mostrados en la FIG. 6 y, por tanto, no se describirá de nuevo en detalle. Con referencia en primer lugar al controlador de sistemas domésticos 1002, un controlador de red doméstico *ad hoc* 1008 controla la formación y terminación de una red doméstica *ad hoc* usando un detector de proximidad 1010 y un controlador de permisos 1012. El controlador de proximidad detecta cualquier dispositivo secundario en comunicación con el controlador de sistemas domésticos 1002 a través de un controlador de comunicación 1014 (que tiene una antena 1016) tal como detectando dispositivos dentro de la casa, dentro de habitaciones particulares o la casa, o dentro de los terrenos de la casa. El controlador de comunicación 1014 puede ser un controlador de punto de acceso doméstico. Además, típicamente, lo general, los diversos dispositivos secundarios del propietario y otros ocupantes permanentes de la casa están prerregistrados para que el controlador de sistemas domésticos pueda agregar o quitar automáticamente los dispositivos de la red *ad hoc* a medida que se llevan hacia y desde la casa durante el transcurso de un día.

[0044] Suponiendo que un dispositivo secundario particular está dentro de la casa y está prerregistrado, como la tableta del propietario 1004, el dispositivo secundario es invitado a la red *ad hoc* enviando señales de emparejamiento adecuadas a través del controlador de comunicación 1014. Si el propietario u otros ocupantes aún no han sido autentificados en el controlador del sistema doméstico 1002, se puede usar un escáner de huellas dactilares o iris 1010 para introducir características biométricas, que a continuación se autentifican mediante un iris y/o controlador de autentificación de huellas dactilares 1018. El valor de autentificación principal mencionado anteriormente (y otros datos tales como las ID de dispositivo para los diversos dispositivos dentro de la red *ad hoc*) pueden enviarse a continuación a los diversos dispositivos secundarios dentro de la casa. Tenga en cuenta que si el controlador de sistemas domésticos está equipado de esta manera, puede rastrear la entrada y salida de los ocupantes a través de monitores de seguridad y detectar la presencia de un intruso.

[0045] La tableta del propietario 1004 se muestra con un controlador de comunicación 1020 y una antena 1021 para recibir señales del controlador de sistemas domésticos 1002 (ya sea directamente o mediante una red de comunicación intermedia). La tableta del propietario también incluye un controlador de emparejamiento 1022 que responde a cualquier señal de emparejamiento recibida desde el controlador de sistemas domésticos 1002 y envía señales de protocolo de enlace de respuesta para unirse a la red doméstica *ad hoc*. En un ejemplo, siempre que se activa la tableta del propietario 1004, envía una señal que anuncia su presencia, a la que el controlador de sistemas domésticos puede responder. Si se requiere autentificación secundaria con la tableta del propietario 1004 (según se determine en base, por ejemplo, en permisos o reglas recibidas del controlador de sistemas domésticos), dicha autorización secundaria puede realizarse usando una cámara 1024 y un controlador de autorización de reconocimiento facial 1026 y autentificación secundaria. Una vez emparejada con el controlador de sistemas domésticos, la tableta del propietario puede usarse para controlar cómodamente varios sistemas domésticos tales como un termostato y un controlador ambiental 1028, un sistema de seguridad 1030 y un sistema de entretenimiento y medios domésticos 1032.

[0046] La tableta del invitado 1006 incluye componentes similares a los de la tableta del propietario, pero estará restringida a los sistemas domésticos del controlador. En breve, la tableta del invitado tiene un controlador de comunicación 1034, una antena 1036 y un controlador de emparejamiento 1038 (así como otros componentes para implementar las funciones del monitor de salud, no mostrados). Si se requiere autentificación secundaria, la autorización secundaria puede realizarse usando una cámara 1040 para detectar una imagen facial y un controlador de autorización de reconocimiento facial 1042 y que realiza la autentificación secundaria. Aunque la FIG. 10 solo muestra la tableta de un propietario y una tableta del invitado; los dispositivos secundarios adicionales o alternativos pueden formar la red *ad hoc* del hogar, incluida la ropa inteligente, los dispositivos de juego de monitores de salud y otros dispositivos móviles de función completa, como tabletas u otros teléfonos inteligentes.

[0047] La FIG. 11 ilustra componentes seleccionados de dispositivos dentro de una red *ad hoc* 1100 basada en un vehículo a modo de ejemplo donde el dispositivo principal es un ordenador de la consola del vehículo 1102 y entre los dispositivos secundarios se incluyen un teléfono inteligente 1104 del propietario y una tableta del invitado 1106. Solo los componentes internos pertinentes a la red *ad hoc* se muestran dentro de los distintos dispositivos. Algunos de los componentes son iguales o similares a los mostrados en la FIG. 10 y, por tanto, no se describirá de nuevo en detalle. Con referencia en primer lugar al ordenador de la consola del vehículo 1102, un controlador de red *ad hoc* del vehículo 1108 controla la formación y terminación de una red del vehículo *ad hoc* usando un detector de proximidad 1110 y un controlador de permisos 1112. El controlador de proximidad detecta cualquier dispositivo secundario en comunicación con el ordenador de la consola del vehículo 1102 a través de un controlador de comunicación 1114 (que tiene una antena 1115) tal como detectando dispositivos dentro del vehículo o cerca. El controlador de comunicación 1114 puede ser un controlador de punto de acceso de vehículo. Además, típicamente, los diversos dispositivos secundarios del propietario del vehículo y los miembros de la familia están prerregistrados para que el ordenador de la consola del vehículo pueda agregar o quitar automáticamente los dispositivos de la red *ad hoc* a medida que entran y salen del vehículo durante el transcurso de la operación. al día, sobre todo si el vehículo es el familiar.

[0048] Suponiendo que un dispositivo secundario particular está dentro del vehículo y está prerregistrado,

como el teléfono inteligente 1104 del propietario, el dispositivo secundario es invitado a la red *ad hoc* enviando señales de emparejamiento adecuadas. Si el propietario aún no ha sido autentificado en el ordenador de la consola del vehículo 1102, se puede usar un escáner 1116 de huellas dactilares, que a continuación se autentifica mediante el controlador de autentificación de huellas dactilares 1118. El valor de autentificación principal mencionado anteriormente (y otros datos tales como las ID de dispositivo para los diversos dispositivos dentro de la red *ad hoc*) pueden enviarse a continuación a los diversos dispositivos secundarios dentro del vehículo.

[0049] Se muestra que el teléfono inteligente 1104 del propietario tiene un controlador de comunicación 1120 y una antena 1121 para recibir señales del controlador de sistemas domésticos 1102 (ya sea directamente o mediante una red de comunicación intermedia). El teléfono inteligente del propietario también incluye un controlador de emparejamiento 1122 que responde a cualquier señal de emparejamiento recibida desde el ordenador de la consola del vehículo 1102 y envía señales de protocolo de enlace de respuesta para unirse a la red *ad hoc* del vehículo. Si se requiere autentificación secundaria con el teléfono inteligente 1104 del propietario (según se determine basándose, por ejemplo, en permisos o reglas recibidas del controlador de sistemas domésticos), dicha autorización secundaria se puede realizar usando una cámara 1124 y un controlador de autorización de reconocimiento facial 1126 y que realiza la autentificación secundaria. Una vez emparejado con el ordenador de la consola del vehículo, el teléfono inteligente del propietario se puede usar para controlar cómodamente varios sistemas del vehículo tales como un termostato y/o controlador ambiental 1128, un sistema de seguridad 1130 y un sistema multimedia y de entretenimiento del vehículo 1132. La tableta del invitado 1106 incluye componentes similares a los del teléfono inteligente 1104 del propietario, pero no podrá controlar los sistemas del vehículo. En resumen, la tableta del invitado tiene un controlador de comunicación 1134, una antena 1136 y un controlador de emparejamiento 1138. Aunque la FIG. 11 solo muestra un teléfono inteligente y una tableta, los dispositivos secundarios adicionales o alternativos pueden formar la red *ad hoc* del vehículo, incluidos varios otros dispositivos móviles de función completa, como otras tabletas, dispositivos de juego u otros teléfonos inteligentes.

[0050] Volviendo ahora a las FIGS. 12 y 13, se describirán diagramas de flujo adicionales que ilustran las operaciones de los dispositivos principales y secundarios. En estos dos diagramas de flujo, las operaciones de un dispositivo principal se muestran con bloques sombreados, mientras que las operaciones de un dispositivo secundario se muestran en bloques sin sombrear. En su lugar, al menos algunas de las funciones del dispositivo secundario pueden ser realizadas por el dispositivo principal, y viceversa, y por lo tanto el diagrama de flujo representa solo un ejemplo de la manera en que las funciones pueden distribuirse entre dispositivos principales y secundarios.

[0051] La FIG. 12 ilustra los procedimientos de autentificación 1200. La autentificación comienza en 1202 seguida por el dispositivo principal en espera de los datos de autentificación biométrica 1204, que se reciben desde el bloque de datos biométricos 1206. Como ya se explicó, el usuario puede introducir parámetros biométricos a través de un escáner de huellas dactilares o similar. Los parámetros biométricos se almacenan con el dispositivo dentro de una base de datos como se muestra en el bloque de datos 1206. El dispositivo principal realiza la autentificación de usuario 1208 para generar un valor de autentificación principal o nivel de confianza 1210. El valor de autentificación biométrica se mapea a un valor de autentificación de dispositivo emparejado (es decir, secundario) basado en un estado de emparejamiento 1212. El estado de emparejamiento puede indicar simplemente si un dispositivo secundario particular está emparejado actualmente con el dispositivo principal a través de un procedimiento de emparejamiento previo 1214. Es decir, mientras el dispositivo principal está esperando datos biométricos en 1204, el dispositivo principal también detecta cualquier dispositivo emparejado 1214 basándose en datos de sensores de posición, redes de comunicación, etc., como ya se describió anteriormente.

[0052] Suponiendo que se encuentra un dispositivo secundario emparejado 1218, entonces el dispositivo emparejado identifica uno o más procedimientos de autentificación para el dispositivo emparejado 1220, tales como procedimientos de reconocimiento facial o de movimiento. El dispositivo secundario emparejado identifica entonces los correspondientes sensores de autentificación secundaria 1222, como un acelerómetro para movimiento, una cámara para imágenes o un micrófono para reconocimiento de voz. El dispositivo secundario emparejado también determina si se requiere la autentificación secundaria 1224 usando técnicas descritas anteriormente tales como examinar permisos o reglas recibidas del dispositivo principal. Suponiendo que se requiere autentificación secundaria, entonces el dispositivo emparejado realiza la autentificación secundaria 1226 basándose en los datos recibidos del bloque 1228, como los datos de la cámara, el acelerómetro o el micrófono. El dispositivo secundario emparejado combina la autentificación biométrica del dispositivo principal (a través del bloque 1210) con la autentificación secundaria del dispositivo emparejado 1230 (es decir, local). El valor combinado resultante se almacena como un valor 1232 de autentificación de dispositivo emparejado final. De forma alternativa, si no se requiere autentificación secundaria en 1224, entonces el dispositivo emparejado avanza a través del bloque 1212 para obtener el valor de autentificación mapeado (por ejemplo, puntuación o nivel) del bloque 1210, que a continuación se almacena como el valor emparejado final. En cualquier caso, la autentificación finaliza 1234.

[0053] La FIG. 13 ilustra los procedimientos de desautentificación 1300. La desautentificación comienza 1302 con el dispositivo principal esperando un activador de desautentificación principal 1304, que se recibe desde el bloque de activador de desautentificación 1306. Como ya se explicó, tales desencadenantes principales de desautentificación pueden involucrar tiempos de espera, intervención manual del usuario y datos de sensores auxiliares (como sensores que indican una diferencia en el ruido ambiental o la luz entre los dispositivos de la red *ad hoc*). Una vez que se recibe un desencadenante de desautentificación principal, el estado de desautentificación del dispositivo principal se establece en "verdadero" 1308, es decir, el dispositivo principal se desautentifica de la red *ad hoc* (y la red *ad hoc* en sí se termina así). Al mismo tiempo, el dispositivo emparejado secundario actualiza su estado de emparejamiento 1310 basándose en la información recibida de los sensores de posición, enlaces de comunicación, señales de emparejamiento, etc., 1312. Suponiendo que el dispositivo secundario permanece emparejado con el dispositivo principal, 1314, el dispositivo secundario espera los activadores 1316 de desautentificación. Entre los activadores de desautentificación recibidos por el dispositivo secundario pueden incluirse los mismos activadores de desautentificación recibidos por el dispositivo principal (a través del bloque 1306) y/o los activadores de desautentificación específicos del dispositivo secundario (a través del bloque 1318). Una vez que se recibe un desencadenante de desautentificación secundaria, el estado de desautentificación del dispositivo secundario se establece en "verdadero" 1320, es decir, el dispositivo secundario se desautentifica de la red *ad hoc* (aunque la red *ad hoc* en sí puede continuar con otros dispositivos secundarios suponiendo que el dispositivo principal tampoco está desautentificado). A la inversa, si el dispositivo secundario determina que ya no está emparejado con el dispositivo principal 1314, entonces el estado de desautentificación del dispositivo secundario se establece igualmente en "verdadero" 1322, es decir, el dispositivo secundario se desautentifica de la red *ad hoc*. Además, el dispositivo secundario puede detectar cualquier amenaza al dispositivo principal, 1324, como las amenazas de piratería o suplantación de identidad mencionadas anteriormente. Si se detecta tal amenaza, un comando de control de seguridad del dispositivo principal se establece en "verdadero" en 1326. Este comando se transmite al dispositivo principal y representa uno de los desencadenantes de desautentificación del dispositivo principal del bloque 1304. En última instancia, la desautentificación finaliza en 1328 después de la desautentificación de un dispositivo secundario o tanto del dispositivo secundario como del dispositivo principal.

Otros sistemas y aparatos a modo de ejemplo

[0054] La FIG. 14 ilustra un sistema o aparato global 1400 en el que pueden implementarse los componentes y procedimientos del dispositivo principal de las FIGS. 2 - 13. De acuerdo con diversos aspectos de la divulgación, puede implementarse un elemento, o cualquier parte de un elemento, o cualquier combinación de elementos, con un sistema de procesamiento 1414 que incluya uno o más circuitos de procesamiento 1404 como el circuito de procesamiento SoC de la FIG. 5. Por ejemplo, el aparato 1400 puede ser un equipo de usuario (UE) de un sistema de comunicación móvil. El aparato 1400 se puede utilizar con un controlador de red de radio (CRR). Además de un SoC, ejemplos de circuitos de procesamiento 1404 incluyen microcircuitos de procesamiento, microcontroladores, circuitos de procesamiento de señales digitales (DSP), matrices de puertas programables por campo (FPGA), dispositivos de lógica programable (PLD), máquinas de estados, lógica de puertas, circuitos de hardware discretos y demás hardware adecuado configurado para implementar las diversas funcionalidades descritas a lo largo de esta divulgación. Es decir, el circuito de procesamiento 1404, como se utiliza en el aparato 1400, puede usarse para implementar uno o más de los procesos descritos anteriormente e ilustrados en las FIGS. 2 a 13 (y los ilustrados en las FIGS. 17 y 18, que se analizan a continuación), como los procesos para realizar la autentificación de usuario basada en datos biométricos.

[0055] En este ejemplo, el sistema de procesamiento 1414 se puede implementar con una arquitectura de bus, representada, en general, por el bus 1402. El bus 1402 puede incluir un número cualquiera de buses y puentes de interconexión dependiendo de la aplicación específica del sistema de procesamiento 1414 y de las restricciones de diseño globales. El bus 1402 conecta varios circuitos, incluyendo uno o más circuitos de procesamiento (representados de manera general mediante el circuito de procesamiento 1404), el dispositivo de almacenamiento 1405 y un medio legible por máquina, legible por circuito de procesamiento o legible por ordenador (representado de manera general por un medio legible por máquina no transitorio 1406). El bus 1402 también puede enlazar otros diversos circuitos, tales como fuentes de temporización, dispositivos periféricos, reguladores de voltaje y circuitos de gestión de potencia, que son bien conocidos en la técnica y que, por lo tanto, no se describirán en mayor detalle. La interfaz de bus 1408 proporciona una interfaz entre el bus 1402 y un transceptor 1410. El transceptor 1410 proporciona un medio para comunicarse con otros diversos aparatos a través de un medio de transmisión. Dependiendo de la naturaleza del aparato, también se puede proporcionar una interfaz de usuario 1412 (por ejemplo, un teclado, un dispositivo de visualización, un altavoz, un micrófono, una palanca de mando).

[0056] El circuito de procesamiento 1404 se encarga de gestionar el bus 1402 y el procesamiento general, incluyendo la ejecución de software almacenado en el soporte legible por máquina 1406. Cuando es ejecutado por el procesador 1404, el software hace que el sistema de procesamiento 1414 lleve a cabo las diversas funciones descritas en el presente documento para cualquier aparato particular. El medio legible por máquina 1406 se puede usar también para almacenar los datos que son manipulados por el circuito de procesamiento 1404 cuando ejecuta el software.

[0057] Uno o más circuitos de procesamiento 1404 del sistema de procesamiento pueden ejecutar software. Se deberá interpretar en términos generales que software quiere decir instrucciones, conjuntos de instrucciones, código, segmentos de código, código de programa, programas, subprogramas, módulos de software, aplicaciones, aplicaciones de software, paquetes de software, rutinas, subrutinas, objetos, módulos ejecutables, hilos de ejecución, procedimientos, funciones, etc., independientemente de si se denomina software, firmware, middleware, microcódigo, lenguaje de descripción de hardware o de otro modo. Un circuito de procesamiento puede realizar las tareas necesarias. Un segmento de código puede representar un procedimiento, una función, un subprograma, un programa, una rutina, una subrutina, un módulo, un paquete de programa informático, una clase o cualquier combinación de instrucciones, estructuras de datos o sentencias de programa. Un segmento de código se puede acoplar a otro segmento de código o a un circuito de hardware pasando y/o recibiendo información, datos, argumentos, parámetros o contenidos de memoria o de almacenamiento. Se puede pasar, enviar o transmitir información, argumentos, parámetros, datos, etc. por medio de cualquier medio adecuado, incluido la compartición de memoria, el paso de mensajes, el paso de testigos, la transmisión por red, etc.

[0058] El software puede residir en un medio legible por ordenador 1406. El medio legible por ordenador 1406 puede ser un medio legible por ordenador no transitorio. Un medio legible por circuito de procesamiento no transitorio, un medio legible por procesador, un medio legible por máquina o un medio legible por ordenador incluye, a modo de ejemplo, un dispositivo de almacenamiento magnético (por ejemplo, un disco duro, un disco flexible, una cinta magnética), un disco óptico (por ejemplo., un disco compacto (CD), un disco versátil digital (DVD)), una tarjeta inteligente, un dispositivo de memoria flash (por ejemplo, una tarjeta, un lápiz USB o un pen drive), una RAM, una ROM, una ROM programable (PROM), una PROM borrable (EPROM), una PROM borrable eléctricamente (EEPROM), un registro, un disco extraíble, un disco duro, un CD-ROM y cualquier otro medio adecuado para almacenar software y/o instrucciones a los que pueda acceder y que pueda leer un ordenador. Las expresiones "medio legible a máquina", "medio legible por ordenador", "medio legible por circuito de procesamiento" y/o "medio legible por procesador" pueden incluir, aunque sin limitación, medios no transitorios como dispositivos de almacenamiento fijos o portátiles, dispositivos de almacenamiento óptico y otros medios diferentes capaces de almacenar, contener o transportar instrucciones y/o datos. Por lo tanto, los diversos procedimientos descritos en el presente documento pueden implementarse parcial o completamente mediante instrucciones y/o datos que pueden almacenarse en un "medio legible por máquina", "medio legible por ordenador", un "medio legible por circuito de procesamiento" y/o un "medio legible por procesador" y ser ejecutados por uno o más circuitos, máquinas y/o dispositivos de procesamiento. El medio legible por máquina también puede incluir, a modo de ejemplo, una onda portadora, una línea de transmisión y cualquier otro medio que sea adecuado para transmitir software y/o instrucciones a los que pueda acceder y leer un ordenador. El medio legible por máquina 1406 puede residir en el sistema de procesamiento 1414, ser externo al sistema de procesamiento 1414 o distribuirse en múltiples entidades que incluyan el sistema de procesamiento 1414. El medio legible por ordenador 1406 puede incorporarse en un producto de programa informático. A modo de ejemplo, un producto de programa informático puede incluir un medio legible por circuito de procesamiento en materiales de embalaje. Los expertos en la técnica reconocerán cómo implementar de la mejor manera la funcionalidad descrita presentada a lo largo de la presente divulgación dependiendo de la aplicación particular y de las limitaciones de diseño globales impuestas en el sistema global.

[0059] En particular, el medio de almacenamiento legible por máquina 1406 puede tener una o más instrucciones que, cuando se ejecutan mediante el circuito de procesamiento 1404, hacen que el circuito de procesamiento: obtenga al menos un parámetro biométrico representativo del usuario del dispositivo principal; determine un valor de autentificación principal representativo de un grado de autentificación del usuario del dispositivo principal basándose en el al menos un parámetro biométrico; autentifique al usuario del dispositivo principal basándose en el valor de autentificación principal; y comparta el valor de autentificación principal con un dispositivo secundario de la red *ad hoc*.

[0060] Uno o más de los componentes, pasos, características y/o funciones ilustrados en las figuras se pueden reorganizar y/o combinar en un solo componente, paso, característica o función o incorporarse en diversos componentes, pasos o funciones. También se pueden añadir elementos, componentes, pasos y/o funciones adicionales sin apartarse de las características y los aspectos descritos. Los aparatos, dispositivos y/o componentes ilustrados en las figuras pueden configurarse para realizar uno o más de los procedimientos, características o pasos que se describen en las figuras. Los algoritmos descritos en el presente documento también pueden implementarse eficientemente en software y/o integrarse eficientemente en hardware.

[0061] Los diversos bloques lógicos, módulos, circuitos, elementos y/o componentes ilustrativos descritos en relación con los ejemplos divulgados en el presente documento pueden implementarse o realizarse con un circuito de procesamiento de propósito general, un circuito de procesamiento de señales digitales (DSP), un circuito integrado de aplicación específica (ASIC), una matriz de puertas de campo programable (FPGA) u otro componente de lógica programable, una lógica de transistores o de puertas discretas, componentes de hardware discretos o cualquier combinación de los mismos diseñada para realizar las funciones descritas en el presente documento. Un procesador de propósito general puede ser un microprocesador, pero, de forma

alternativa, el procesador puede ser cualquier procesador, controlador, microcontrolador o máquina de estado convencional. Un circuito de procesamiento también puede implementarse como una combinación de componentes informáticos, por ejemplo una combinación de un circuito DSP y un microprocesador, varios microcircuitos de procesamiento, uno o más microcircuitos de procesamiento en conjunción con un núcleo de DSP o cualquier otra configuración de este tipo.

[0062] Por tanto, en un aspecto de la divulgación, el circuito de procesamiento 500 y/o 1404 ilustrado en las FIGS. 5 y 14, respectivamente, puede ser un circuito de procesamiento especializado (por ejemplo, un ASIC)) que está específicamente diseñado y/o cableado para realizar los algoritmos, procedimientos y/o pasos descritos en las FIGS. 4, 7, 8, 12 y/o 13 (y/o las FIGS.17 y 18, analizadas a continuación). Por tanto, dicho circuito de procesamiento especializado (por ejemplo., un circuito ASIC) puede ser un ejemplo de un medio para ejecutar los algoritmos, procedimientos y/o pasos descritos en las FIGS. 4, 7, 8, 12 y/o 13 (y/o las FIGS. 17 y 18 analizadas a continuación). El medio de almacenamiento legible por máquina puede almacenar instrucciones que, cuando sean ejecutadas por un circuito de procesamiento especializado (por ejemplo, un circuito ASIC), hagan que el circuito de procesamiento especializado realice los algoritmos, procedimientos y/o pasos descritos en el presente documento.

[0063] La FIG. 15 ilustra componentes seleccionados y a modo de ejemplo del circuito de procesamiento 1404 de un dispositivo principal de una red *ad hoc*. En particular, el circuito de procesamiento 1404 de la FIG. 15 incluye un módulo/circuito 1500 de determinación del grado de autentificación configurado para determinar un valor de autentificación principal representativo de un grado de autentificación del usuario del dispositivo principal basándose en el al menos un parámetro biométrico. El parámetro biométrico puede ser detectado por un detector de parámetro biométrico principal 1502, que está configurado para obtener al menos un parámetro biométrico representativo del usuario del dispositivo principal. El circuito de procesamiento 1404 también incluye: un módulo/circuito de autentificación de usuario 1504 configurado para autentificar al usuario del dispositivo principal basándose en el valor de autentificación principal; un módulo/circuito 1506 de intercambio de autentificación principal configurado para compartir el valor de autentificación principal con un dispositivo secundario de la red *ad hoc* a través de un circuito/módulo de comunicación de red 1514 *ad hoc*; y un módulo/circuito de desautentificación del dispositivo principal 1508 configurado para detectar un activador para desautentificar al usuario del dispositivo principal y, en respuesta, desautentificar al usuario del dispositivo principal y al dispositivo secundario de la red *ad hoc* en el que el activador para desautentificar al usuario del dispositivo principal puede incluir al menos uno de: (a) una desautentificación del dispositivo principal iniciada por un usuario, (b) un tiempo de espera del dispositivo principal, o (c) una indicación de amenaza del dispositivo principal representativa de un compromiso de seguridad del dispositivo principal.

[0064] El circuito de procesamiento 1404 también incluye: un módulo/circuito 1510 de desautentificación del dispositivo secundario configurado para detectar un activador para desautentificar al usuario del dispositivo secundario y, en respuesta, enviar una señal al dispositivo secundario para desautentificar al usuario del dispositivo secundario, en el que el activador para desautentificar al usuario del dispositivo secundario incluye al menos uno de: (a) una desautentificación del dispositivo secundario iniciada por un usuario, (b) un tiempo de espera del dispositivo secundario, (c) una indicación de amenaza del dispositivo secundario representativa de un compromiso de seguridad del dispositivo secundario, (d) una pérdida de comunicación con el dispositivo secundario, (e) una pérdida de elementos comunes entre el dispositivo principal y el dispositivo secundario, o (f) una violación de una política de permisos predeterminada. El circuito de procesamiento 1404 también incluye: un módulo/circuito de formación/terminación de red *ad hoc* 1512 configurado para formar y posteriormente terminar una red *ad hoc* basada en señales enviadas y recibidas a través del módulo/circuito de comunicación de red *ad hoc* 1514; un módulo/circuito de detección de elementos comunes de dispositivo 1516 configurado para detectar una pérdida de elementos comunes entre el dispositivo principal y el dispositivo secundario basándose en una pérdida de elementos comunes en uno o más de ruido ambiental, luz ambiental, ubicación, movimiento y un enlace de comunicación compartido; y un módulo/circuito 1518 de permisos/políticas de agrupación configurado para administrar políticas y permisos de red *ad hoc*. También pueden proporcionarse otros componentes y la ilustración de la FIG. 15 no es de ninguna manera exhaustiva.

[0065] La FIG. 16 ilustra componentes de instrucción seleccionados y a modo de ejemplo del medio 1406 legible por máquina o legible por ordenador. En particular, el medio legible por máquina 1406 de la FIG. 16 incluye instrucciones 1600 de determinación del grado de autentificación, que cuando son ejecutadas por el circuito de procesamiento de la FIG. 15, hacen que el circuito de procesamiento determine un valor de autentificación principal representativo de un grado de autentificación del usuario del dispositivo principal basándose en el al menos un parámetro biométrico. El parámetro biométrico puede detectarse usando las instrucciones 1602 de detección del parámetro biométrico principal, que están configuradas/operativas para obtener al menos un parámetro biométrico representativo del usuario del dispositivo principal. El medio legible por máquina 1406 también incluye: unas instrucciones de autentificación de usuario 1604 configuradas/operativas para autentificar al usuario del dispositivo principal basándose en el valor de autentificación principal; instrucciones de uso compartido de autentificación principal 1606 configuradas/operativas para compartir el valor de autentificación principal con un dispositivo secundario de la red *ad hoc* a través de instrucciones de comunicación de red *ad hoc* 1614; e instrucciones de desautentificación

del dispositivo principal 1608 configuradas/operativas para detectar un activador para desautentificar al usuario del dispositivo principal y, en respuesta, desautentificar al usuario del dispositivo principal y al dispositivo secundario de la red *ad hoc* en el que el activador para desautentificar al usuario del dispositivo principal puede incluir al menos uno de: (a) una desautentificación del dispositivo principal iniciada por un usuario, (b) un tiempo de espera del dispositivo principal, o (c) una indicación de amenaza del dispositivo principal representativa de un compromiso de seguridad del dispositivo principal.

[0066] El medio legible por máquina 1406 también incluye instrucciones 1610 de desautentificación del dispositivo secundario configuradas/operativas para detectar un activador para desautentificar al usuario del dispositivo secundario y, en respuesta, enviar una señal al dispositivo secundario para desautentificar al usuario del dispositivo secundario, en el que el activador para desautentificar al usuario del dispositivo secundario incluye al menos uno de: (a) una desautentificación del dispositivo secundario iniciada por un usuario, (b) un tiempo de espera del dispositivo secundario, (c) una indicación de amenaza del dispositivo secundario representativa de un compromiso de seguridad del dispositivo secundario, (d) una pérdida de comunicación con el dispositivo secundario, (e) una pérdida de elementos comunes entre el dispositivo principal y el dispositivo secundario, o (f) una violación de una política de permisos predeterminada. El medio legible por máquina 1406 también incluye: instrucciones de formación/terminación de red *ad hoc* 1612 configuradas/operativas para formar y posteriormente terminar una red *ad hoc* basada en señales enviadas y recibidas a través de las instrucciones de comunicación de red *ad hoc* 1614; instrucciones de detección de elementos comunes del dispositivo 1616 configuradas/operativas para detectar una pérdida de elementos comunes entre el dispositivo principal y el dispositivo secundario basándose en una pérdida de elementos comunes en al menos uno de ruido ambiental, luz ambiental, ubicación, movimiento o un enlace de comunicación compartido; e instrucciones de agrupación de permisos/políticas 1618 configuradas/operativas para gestionar permisos y políticas de red *ad hoc*. También se pueden proporcionar otras instrucciones y la ilustración de la FIG. 16 no es de ninguna manera exhaustiva.

[0067] La FIG. 17 ilustra y resume ampliamente procedimientos o procesos 1700 que pueden realizarse mediante el circuito de procesamiento 1404 de las FIGS. 14 y 15 u otros dispositivos equipados adecuadamente para su uso mediante un dispositivo principal para la autentificación de un usuario. En 1702, el circuito de procesamiento obtiene al menos un parámetro biométrico representativo del usuario del dispositivo principal y, en 1704, determina un valor de autentificación principal representativo de un grado de autentificación del usuario del dispositivo principal basado en al menos un parámetro biométrico. En 1706, el circuito de procesamiento autentifica al usuario del dispositivo principal basándose en el valor de autentificación principal y, en 1708, comparte el valor de autentificación principal con un dispositivo secundario (por ejemplo, a través de una red *ad hoc*) para facilitar la autentificación del usuario por parte del dispositivo secundario.

[0068] La FIG. 18 ilustra y resume ampliamente procedimientos o procesos 1800 adicionales que se pueden realizar mediante el circuito de procesamiento 1404 de las FIGS. 14 y 15 u otros dispositivos equipados adecuadamente para su uso mediante un dispositivo principal de una red *ad hoc* para la autentificación de un usuario. El circuito de procesamiento puede invitar/cancelar la invitación de dispositivos secundarios a/desde la red *ad hoc* basándose en los elementos comunes (o ausencia de ellos) en al menos uno de ruido ambiental, luz ambiental, ubicación, movimiento o enlaces de comunicación compartidos 1802. El circuito de procesamiento reenvía uno o más permisos y políticas a uno o más dispositivos secundarios junto con el valor de autentificación principal, que puede ser un valor de autentificación (por ejemplo, puntuación o nivel de confianza) 1804. El circuito de procesamiento puede detectar un activador para desautentificar al usuario del dispositivo principal y, en respuesta, desautentifica al usuario del dispositivo principal y todos los dispositivos secundarios de la red *ad hoc*, en el que el activador para desautentificar al usuario del dispositivo principal incluye uno o más de una desautentificación del dispositivo principal iniciada por el usuario, un tiempo de espera del dispositivo principal y una indicación de amenaza del dispositivo principal representativa de un compromiso de seguridad del dispositivo principal 1806. El circuito de procesamiento detecta un activador para desautentificar al usuario de un dispositivo secundario y, en respuesta, envía señales al dispositivo secundario para desautentificar al usuario del dispositivo secundario, en el que el activador para desautentificar al usuario del dispositivo secundario incluye uno o más de una desautentificación del dispositivo secundario iniciada por un usuario, un tiempo de espera del dispositivo secundario, una indicación de amenaza del dispositivo secundario representativa de un compromiso de seguridad del dispositivo secundario, una pérdida de comunicación con el dispositivo secundario, una pérdida de elementos comunes entre el dispositivo principal y el dispositivo secundario y una violación de un permiso o política predeterminados 1808.

[0069] La FIG. 19 ilustra componentes seleccionados y a modo de ejemplo del circuito de procesamiento 1900 de un dispositivo secundario de una red *ad hoc* (que puede tener una arquitectura similar a la del dispositivo principal de la FIG. 14). En particular, el circuito de procesamiento 1900 de la FIG. 19 incluye un módulo/circuito 1902 de recepción de grado de autentificación configurado para recibir y procesar un valor de autentificación principal representativo de un grado de autentificación del usuario del dispositivo principal recibido desde el dispositivo principal usando un circuito/módulo 1908 de comunicación de red *ad hoc*. Un módulo/circuito 1906 de determinación de autentificación secundaria está configurado para determinar si se debe realizar una autentificación secundaria del usuario. Si es así, la autentificación secundaria es realizada o

controlada por un módulo/circuito de autentificación secundaria 1910, que está configurado para obtener al menos un parámetro biométrico usando un detector de parámetro biométrico secundario 1912 representativo del usuario del dispositivo secundario y para determinar una autentificación secundaria. valor representativo de un grado de autentificación del usuario del dispositivo secundario basado en al menos un parámetro biométrico obtenido usando el dispositivo secundario. Un módulo/circuito 1914 de determinación del valor de autentificación combinado final está configurado para combinar el valor de autentificación principal recibido del dispositivo principal con el valor de autentificación secundaria para producir un valor de autentificación combinado. El módulo/circuito de autentificación secundaria 1910 a continuación autentifica al usuario del dispositivo secundario usando el valor de autentificación combinado.

[0070] El circuito de procesamiento 1900 también incluye un módulo/circuito de detección de desautentificación del dispositivo principal 1916 configurado para detectar una indicación de amenaza de dispositivo principal en el dispositivo secundario y para controlar el envío de una señal al dispositivo principal para desautentificar al usuario del dispositivo principal (usando el módulo/circuito de comunicación 1908.) El circuito de procesamiento 1900 también incluye un módulo/circuito 1918 de desautentificación del dispositivo secundario configurado para detectar un activador para desautentificar al usuario del dispositivo secundario y, en respuesta, desautentificar al usuario del dispositivo secundario y notificar al dispositivo principal, en el que el activador para desautentificar al usuario del dispositivo secundario incluye una o más de la desautentificación del dispositivo secundario iniciada por el usuario, un tiempo de espera del dispositivo secundario, una indicación de amenaza del dispositivo secundario representativa de un compromiso de seguridad del dispositivo secundario y una indicación de amenaza del dispositivo principal representativa de un compromiso de seguridad del dispositivo principal. El circuito de procesamiento 1900 también incluye un módulo/circuito 1920 de permisos/políticas de agrupación configurado para administrar permisos y políticas de red *ad hoc* en nombre del dispositivo secundario. También pueden proporcionarse otros componentes y la ilustración de la FIG. 19 no es de ninguna manera exhaustiva.

[0071] La FIG. 20 ilustra componentes de instrucción seleccionados y a modo de ejemplo de un medio legible por máquina 2000 de un dispositivo secundario. En particular, el medio legible por máquina 2000 de la FIG. 20 incluye instrucciones de recepción de grado de autentificación 2002, que cuando son ejecutadas por un circuito de procesamiento del dispositivo secundario, hacen que el circuito de procesamiento reciba y procese un valor de autentificación principal representativo de un grado de autentificación del usuario del dispositivo principal recibido del dispositivo principal utilizando una red *ad hoc* instrucciones de comunicación 2008. Las instrucciones de determinación de autentificación secundaria 2006 están configuradas/operativas para determinar si se debe realizar una autentificación secundaria del usuario. De ser así, la autentificación secundaria se realiza o controla mediante las instrucciones de autentificación secundaria 2010, que son operativas para obtener al menos un parámetro biométrico mediante un detector de parámetro biométrico secundario 2012 representativo del usuario del dispositivo secundario y para determinar un valor de autentificación secundaria representativo de un grado de autentificación del usuario del dispositivo secundario basado en el al menos un parámetro biométrico obtenido usando el dispositivo secundario. Las instrucciones finales de determinación del valor de autentificación combinado 2014 están configuradas/operativas para combinar el valor de autentificación principal recibido del dispositivo principal con el valor de autentificación secundaria para producir un valor de autentificación combinado. A continuación, las instrucciones de autentificación secundaria 2010 autentifican al usuario del dispositivo secundario utilizando el valor de autentificación combinado.

[0072] El medio legible por máquina 2000 también incluye instrucciones 2016 de detección de desautentificación del dispositivo principal configuradas/operativas para detectar una indicación de amenaza de dispositivo principal en el dispositivo secundario y para controlar el envío de una señal al dispositivo principal para desautentificar al usuario del dispositivo principal. El medio 2000 también incluye instrucciones 2018 de desautentificación del dispositivo secundario configuradas/operativas para detectar un activador para desautentificar al usuario del dispositivo secundario y, en respuesta, para desautentificar al usuario del dispositivo secundario y notificar al dispositivo principal, en el que el activador para desautentificar al usuario del dispositivo secundario incluye una o más de una desautentificación de dispositivo secundario iniciada por el usuario, un tiempo de espera de dispositivo secundario, una indicación de amenaza de dispositivo secundario representativa de un compromiso de seguridad del dispositivo secundario y una indicación de amenaza de dispositivo principal representativa de un compromiso de seguridad del dispositivo principal. El medio 2000 también incluye instrucciones de políticas/permisos de agrupación 2020 configuradas/operativas para administrar permisos y políticas de red *ad hoc* en nombre del dispositivo secundario. También se pueden proporcionar otras instrucciones y la ilustración de la FIG. 20 no es en absoluto exhaustiva.

[0073] La FIG. 21 ilustra y resume ampliamente procedimientos o procesos 2100 que pueden realizarse mediante el circuito de procesamiento 1900 de la FIG. 19 u otros dispositivos equipados adecuadamente para su uso mediante un dispositivo secundario para la autentificación de un usuario. El circuito de procesamiento recibe un valor de autentificación principal representativo de un grado de autentificación de un usuario (del dispositivo secundario) desde un dispositivo principal (por ejemplo, a través de una red inalámbrica *ad hoc*) 2102. El circuito de procesamiento determina si se debe realizar una autentificación secundaria del usuario y,

de ser así, entonces (a) obtiene al menos un parámetro biométrico usando el dispositivo secundario representativo del usuario; (b) determina un valor de autentificación secundaria representativo de un grado de autentificación del usuario del dispositivo secundario basándose en el al menos un parámetro biométrico obtenido usando el dispositivo secundario; (c) combina el valor de autentificación principal recibido del dispositivo principal con el valor de autentificación secundaria para producir un valor de autentificación combinado; y (d) autentifica al usuario del dispositivo secundario utilizando el valor de autentificación combinado 2104.

[0074] La FIG. 22 ilustra y resume ampliamente procedimientos o procesos 2200 adicionales que pueden realizarse mediante el circuito de procesamiento 1900 de la FIG. 19 u otros dispositivos equipados adecuadamente para su uso mediante un dispositivo secundario de una red *ad hoc* para la autentificación de un usuario. El circuito de procesamiento recibe señales de invitación/cancelación de invitación de la red *ad hoc* basadas en elementos comunes en al menos uno de los enlaces 2202 de ruido ambiental, luz ambiental, ubicación, movimiento o comunicación compartida y recibe uno o más permisos y políticas para los dispositivos secundarios. junto con el valor de autentificación principal 2204. El circuito de procesamiento determina si se requiere autentificación secundaria basándose en si se requiere una autentificación secundaria basándose en una acción iniciada por el usuario, como una o más de una transacción financiera, acceso a contenido seguro y acceso a sistemas de control seguros y, de ser así, realizar la autentificación secundaria detectando uno o más de un parámetro de reconocimiento de gestos, un parámetro de reconocimiento facial y un parámetro 2206 de reconocimiento de voz. El circuito de procesamiento detecta un activador para desautentificar al usuario del dispositivo secundario y, en respuesta, desautentifica al usuario del dispositivo secundario y notifica al dispositivo principal en el que el activador para desautentificar al usuario del dispositivo secundario incluye uno o más de una desautentificación del dispositivo secundario iniciada por un usuario, un tiempo de espera del dispositivo secundario, una indicación de amenaza del dispositivo secundario representativa de un compromiso de seguridad del dispositivo secundario, una pérdida de comunicación con el dispositivo principal y una violación de un permiso o política predeterminada u otra política de agrupación 2208. El circuito de procesamiento realiza transacciones financieras por cantidades autorizadas que son inferiores a las del dispositivo principal de la red *ad hoc* 2210.

[0075] Se observa que los aspectos de la presente divulgación pueden describirse en el presente documento como un proceso que se representa como un organigrama, un diagrama de flujo, un diagrama estructural o un diagrama de bloques. Aunque un organigrama puede describir las operaciones como un proceso secuencial, muchas de las operaciones pueden realizarse en paralelo o simultáneamente. Además, el orden de las operaciones puede redisponerse. Un proceso se termina cuando se acaban sus operaciones. Un procedimiento puede corresponder a un procedimiento, una función, un procedimiento, una subrutina, un subprograma, etc. Cuando un procedimiento corresponde a una función, su finalización corresponde a un retorno de la función a la función de llamada o a la función principal.

[0076] Los expertos en la técnica apreciarán además que los diversos bloques lógicos, módulos, circuitos y pasos de algoritmo ilustrativos descritos en relación con los aspectos divulgados en el presente documento pueden implementarse como hardware electrónico, software informático o combinaciones de ambos. Para ilustrar claramente esta intercambiabilidad de hardware y programa informático, anteriormente se han descrito en general diversos componentes, bloques, módulos, circuitos y pasos ilustrativos desde el punto de vista de su funcionalidad. Que dicha funcionalidad se implemente como hardware o programa informático depende de la aplicación y las restricciones de diseño en particular impuestas al sistema global.

[0077] Se contempla que las diversas características descritas en el presente documento se pueden implementar en diferentes sistemas. Cabe destacar que los aspectos anteriores de la divulgación son simplemente ejemplos y no han de interpretarse como limitativos. La descripción de los aspectos de la presente divulgación pretende ser ilustrativa y no limitar el alcance de las reivindicaciones. Como tales, las presentes enseñanzas se pueden aplicar fácilmente a otros tipos de aparatos, y muchas alternativas, modificaciones y variaciones serán evidentes para los expertos en la técnica.

REIVINDICACIONES

1. Un procedimiento para la autentificación de un usuario de un dispositivo secundario, operativo mediante el dispositivo secundario en una red inalámbrica personal *ad hoc* que comprende un dispositivo principal y el dispositivo secundario, en el que el dispositivo principal y el dispositivo secundario son transportados o usados por el usuario, el procedimiento comprendiendo:

recibir un valor de autentificación principal representativo de un grado de autentificación del usuario desde el dispositivo principal a través de la red inalámbrica personal *ad hoc*, en el que el valor de autentificación principal indica un grado de coincidencia entre un parámetro biométrico obtenido por un detector de parámetro biométrico del dispositivo principal y características correspondientes de un usuario autorizado del dispositivo principal; y

determinar si se debe realizar una autentificación secundaria del usuario y, si se va a realizar una autentificación secundaria, entonces

(a) obtener al menos un parámetro biométrico representativo del usuario que utiliza el dispositivo secundario utilizando un detector de parámetros biométricos del dispositivo secundario,

(b) determinar un valor de autentificación secundaria representativo de un grado de autentificación del usuario basándose en el al menos un parámetro biométrico obtenido usando el dispositivo secundario,

(c) combinar el valor de autentificación principal recibido del dispositivo principal con el valor de autentificación secundaria para producir un valor de autentificación combinado, y

(d) autentificar al usuario del dispositivo secundario usando el valor de autentificación combinado comparando el valor de autentificación combinado con un umbral.

2. El procedimiento según la reivindicación 1, que incluye además la detección de un activador para desautentificar al usuario del dispositivo secundario y, en respuesta, desautentificar al usuario del dispositivo secundario y notificar al dispositivo principal.

3. El procedimiento según la reivindicación 2, en el que el activador para desautentificar al usuario del dispositivo secundario incluye al menos uno de: (a) una desautentificación del dispositivo secundario iniciada por un usuario, (b) un tiempo de espera del dispositivo secundario, (c) una indicación de amenaza de dispositivo secundario representativa de un compromiso de seguridad del dispositivo secundario, o (d) una indicación de amenaza de dispositivo principal representativa de un compromiso de seguridad del dispositivo principal.

4. El procedimiento según la reivindicación 1:

incluyendo además la detección de una indicación de amenaza del dispositivo principal en el dispositivo secundario y el envío de una señal al dispositivo principal para anular la autentificación del usuario del dispositivo principal; o

en el que obtener al menos un parámetro biométrico usando el dispositivo secundario incluye detectar uno o más de un parámetro de reconocimiento de gestos, un parámetro de reconocimiento facial y un parámetro de reconocimiento de voz; o

en el que el dispositivo principal y el dispositivo secundario están autorizados para realizar transacciones financieras y en el que el dispositivo secundario está autorizado para realizar transacciones financieras solo por cantidades inferiores a las que el dispositivo principal está autorizado a realizar.

5. El procedimiento según la reivindicación 1, en el que el dispositivo secundario determina si se requiere una autentificación secundaria basándose en una acción iniciada por el usuario.

6. El procedimiento de una cualquiera de las reivindicaciones 1 a 5, el procedimiento comprendiendo adicionalmente:

obtener al menos un parámetro biométrico representativo de un usuario del dispositivo principal usando un detector de parámetro biométrico del dispositivo principal;

determinar un valor de autentificación principal representativo de un grado de autentificación del usuario del dispositivo principal basado en al menos un parámetro biométrico, en el que el valor de

autentificación principal indica un grado de coincidencia entre el parámetro biométrico y las características correspondientes de un usuario autorizado del dispositivo;

autentificar al usuario del dispositivo principal basándose en el valor de autentificación principal; y

transmitir el valor de autentificación principal al dispositivo secundario a través de la red inalámbrica personal *ad hoc* para facilitar la autentificación del usuario por parte del dispositivo secundario.

7. El procedimiento según la reivindicación 6, en el que el valor de autentificación principal representativo de un grado de autentificación del usuario es al menos uno de: (a) una puntuación de autentificación, o (b) un nivel de confianza.

8. Un dispositivo secundario para que un usuario lo lleve o use y use en una red inalámbrica personal *ad hoc*, que comprende:

un receptor operativo para recibir un valor de autentificación principal representativo de un grado de autentificación de un usuario desde un dispositivo principal a través de una red inalámbrica personal *ad hoc* que comprende los dispositivos principal y secundario, en el que el valor de autentificación principal indica un grado de coincidencia entre un parámetro biométrico obtenido por un detector de parámetros biométricos del dispositivo principal y características correspondientes de un usuario autorizado del dispositivo principal;

un detector de parámetros biométricos; y

un circuito de procesamiento acoplado al receptor y al detector de parámetros biométricos, con el circuito de procesamiento operativo para determinar si se debe realizar una autentificación secundaria del usuario y adicionalmente operativo , si se va a realizar una autentificación secundaria, para

(a) obtener al menos un parámetro biométrico representativo del usuario del dispositivo secundario utilizando el detector de parámetros biométricos,

(b) determinar un valor de autentificación secundaria representativo de un grado de autentificación del usuario basado en al menos un parámetro biométrico,

(c) combinar el valor de autentificación principal recibido del dispositivo principal con el valor de autentificación secundaria para producir un valor de autentificación combinado, y

(d) autentificar al usuario del dispositivo secundario utilizando el valor de autentificación combinado comparando el valor de autentificación combinado con un umbral.

9. El dispositivo secundario según la reivindicación 8:

(a) en el que el dispositivo secundario es un dispositivo móvil para su uso cerca de un vehículo que tiene un ordenador de control como dispositivo principal;

(b) en el que el dispositivo secundario es un dispositivo móvil para su uso en las proximidades de un edificio que tiene un ordenador de control como dispositivo principal; o

(c) en el que el dispositivo secundario es al menos uno de entre un reloj inteligente, un par de gafas inteligentes, un monitor de salud móvil o un artículo de ropa inteligente para usar cerca de un teléfono inteligente como dispositivo principal.

10. Un sistema de autentificación que comprende el dispositivo secundario según la reivindicación 8 o la reivindicación 9, y un dispositivo principal para que un usuario lo lleve o lo lleve puesto y use en la red inalámbrica personal *ad hoc*, comprendiendo el dispositivo principal:

un detector de parámetros biométricos configurado para obtener al menos un parámetro biométrico representativo de un usuario de un dispositivo principal;

un transmisor; y

un circuito de procesamiento acoplado al detector de parámetros biométricos y al transmisor, con el circuito de procesamiento configurado para

determinar un valor de autentificación principal representativo de un grado de autentificación del usuario del dispositivo principal basado en al menos un parámetro biométrico, en el que el valor

de autentificación principal indica un grado de coincidencia entre el parámetro biométrico y las características correspondientes de un usuario autorizado del dispositivo,

autentificar al usuario del dispositivo principal basándose en el valor de autentificación principal, y

transmitir el valor de autentificación principal al dispositivo secundario a través de una red inalámbrica personal *ad hoc* que comprende los dispositivos principal y secundario utilizando el transmisor para facilitar la autentificación del usuario por parte del dispositivo secundario.

11. El sistema de autentificación según la reivindicación 10:

(a) en el que el dispositivo principal es un ordenador de control de un vehículo y el dispositivo secundario es un dispositivo móvil en las proximidades del vehículo;

(b) en el que el dispositivo principal es un ordenador de control de un edificio y el dispositivo secundario es un dispositivo móvil en las proximidades del edificio; o

(c) en el que el dispositivo principal es un teléfono inteligente y el dispositivo secundario es al menos uno de entre un reloj inteligente, un par de gafas inteligentes, un monitor de salud móvil o un artículo de ropa inteligente.

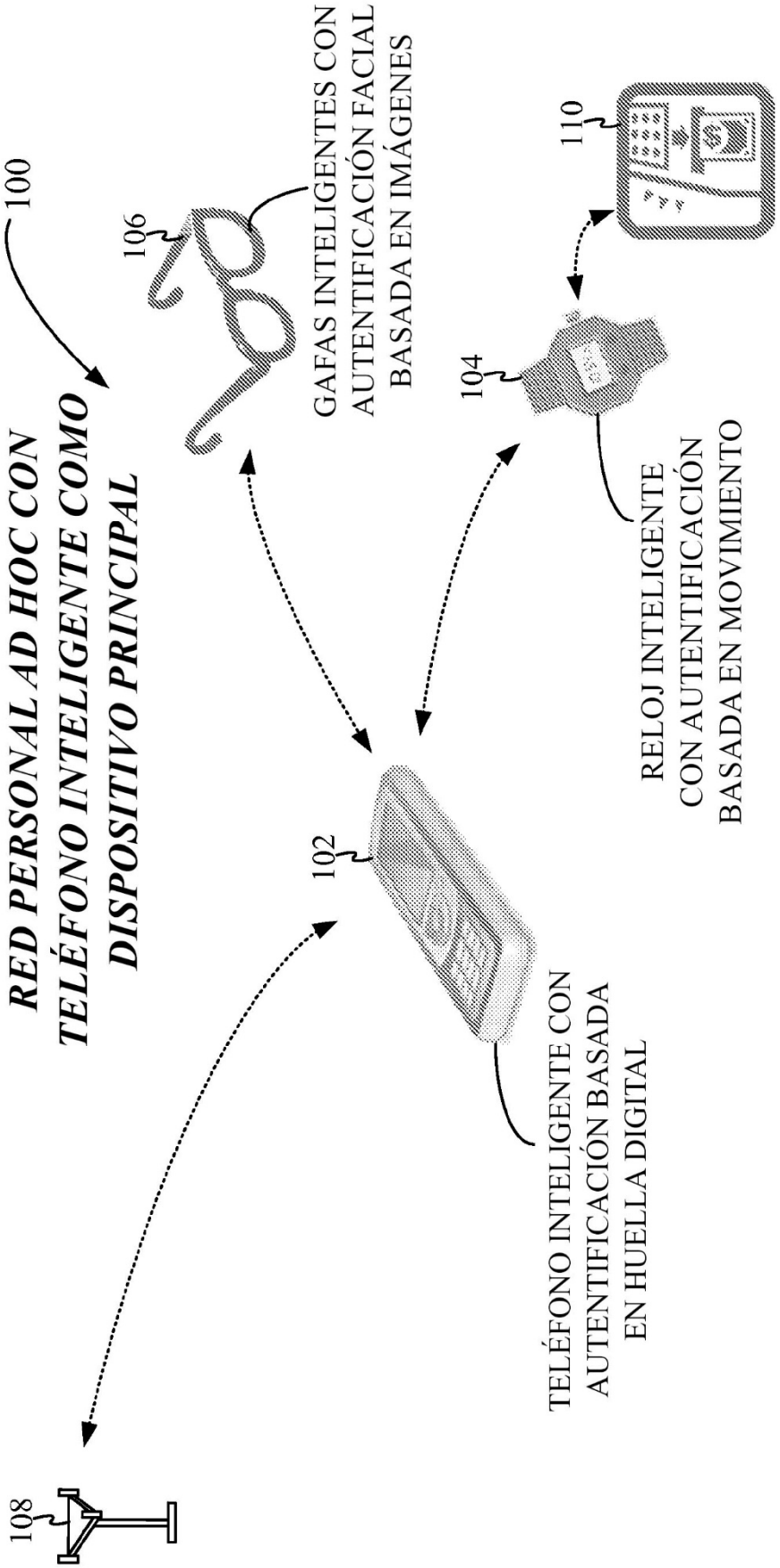
RED PERSONAL AD HOC CON TELÉFONO INTELIGENTE COMO DISPOSITIVO PRINCIPAL
100
106
GAFAS INTELIGENTES CON AUTENTIFICACIÓN FACIAL BASADA EN IMÁGENES
110
104
RELOJ INTELIGENTE CON AUTENTIFICACIÓN BASADA EN MOVIMIENTO
102
TELÉFONO INTELIGENTE CON AUTENTIFICACIÓN BASADA EN HUELLA DIGITAL
108

FIG. 1

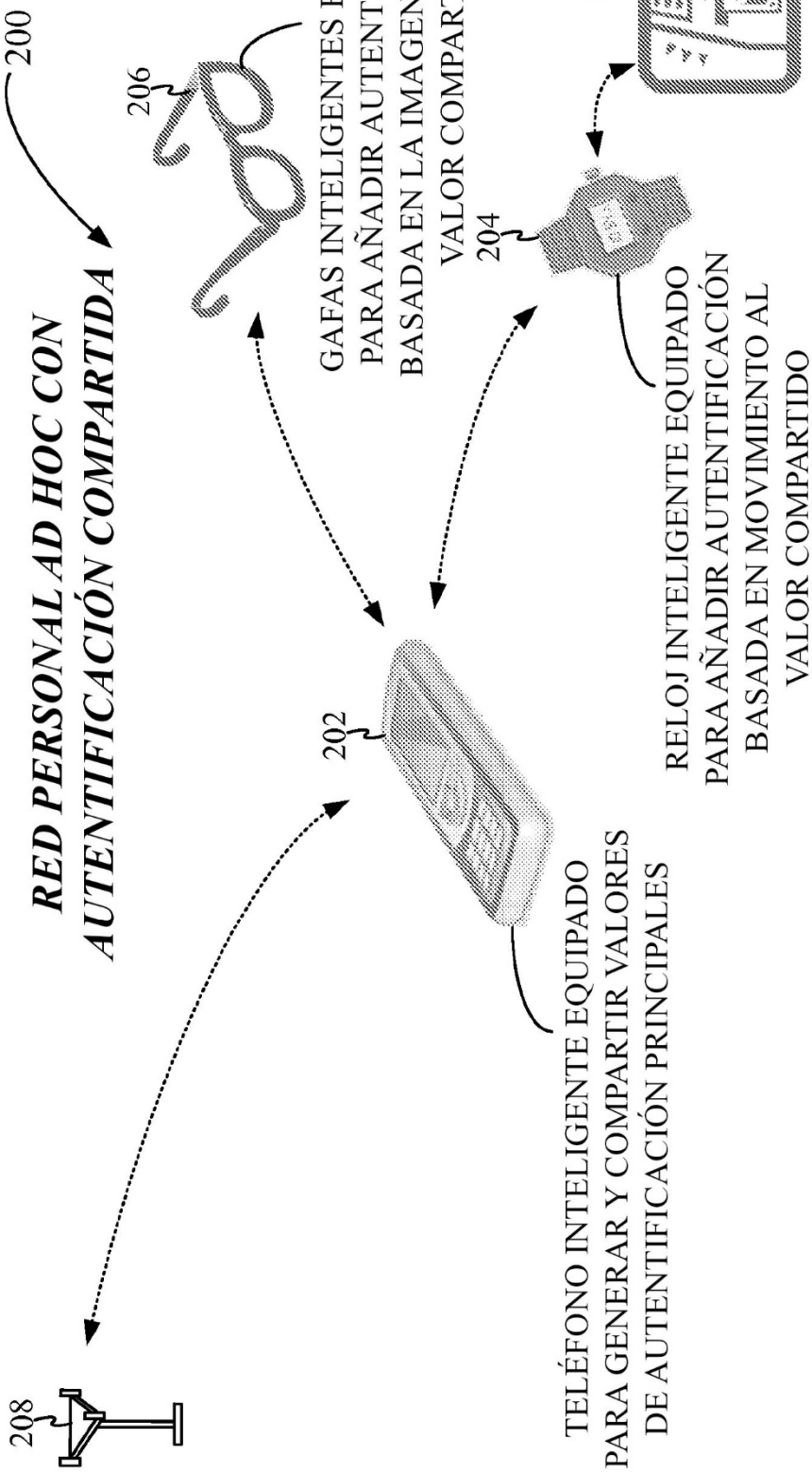
RED PERSONAL AD HOC CON AUTENTIFICACIÓN COMPARTIDA
200
206
GAFAS INTELIGENTES EQUIPADAS PARA AÑADIR AUTENTIFICACIÓN BASADA EN LA IMAGEN FACIAL AL VALOR COMPARTIDO
204
210
RELOJ INTELIGENTE EQUIPADO PARA AÑADIR AUTENTIFICACIÓN BASADA EN MOVIMIENTO AL VALOR COMPARTIDO
202
TELÉFONO INTELIGENTE EQUIPADO PARA GENERAR Y COMPARTIR VALORES DE AUTENTIFICACIÓN PRINCIPALES
208

FIG. 2

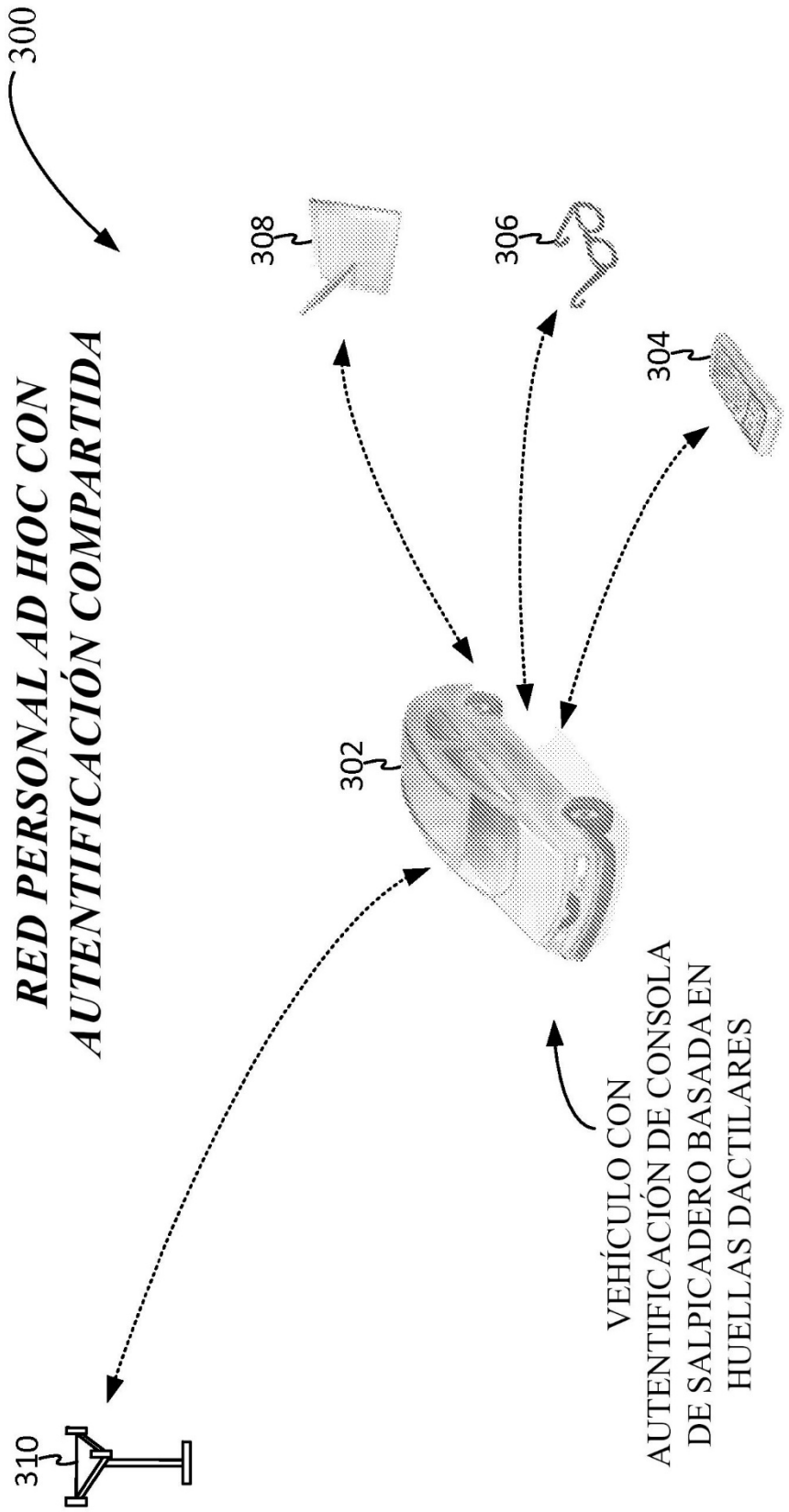
300
RED PERSONAL AD HOC CON AUTENTIFICACIÓN COMPARTIDA
308
306
304
302
310
VEHÍCULO CON AUTENTIFICACIÓN DE CONSOLA DE SALPICADERO BASADA EN HUELLAS DACTILARES

FIG. 3

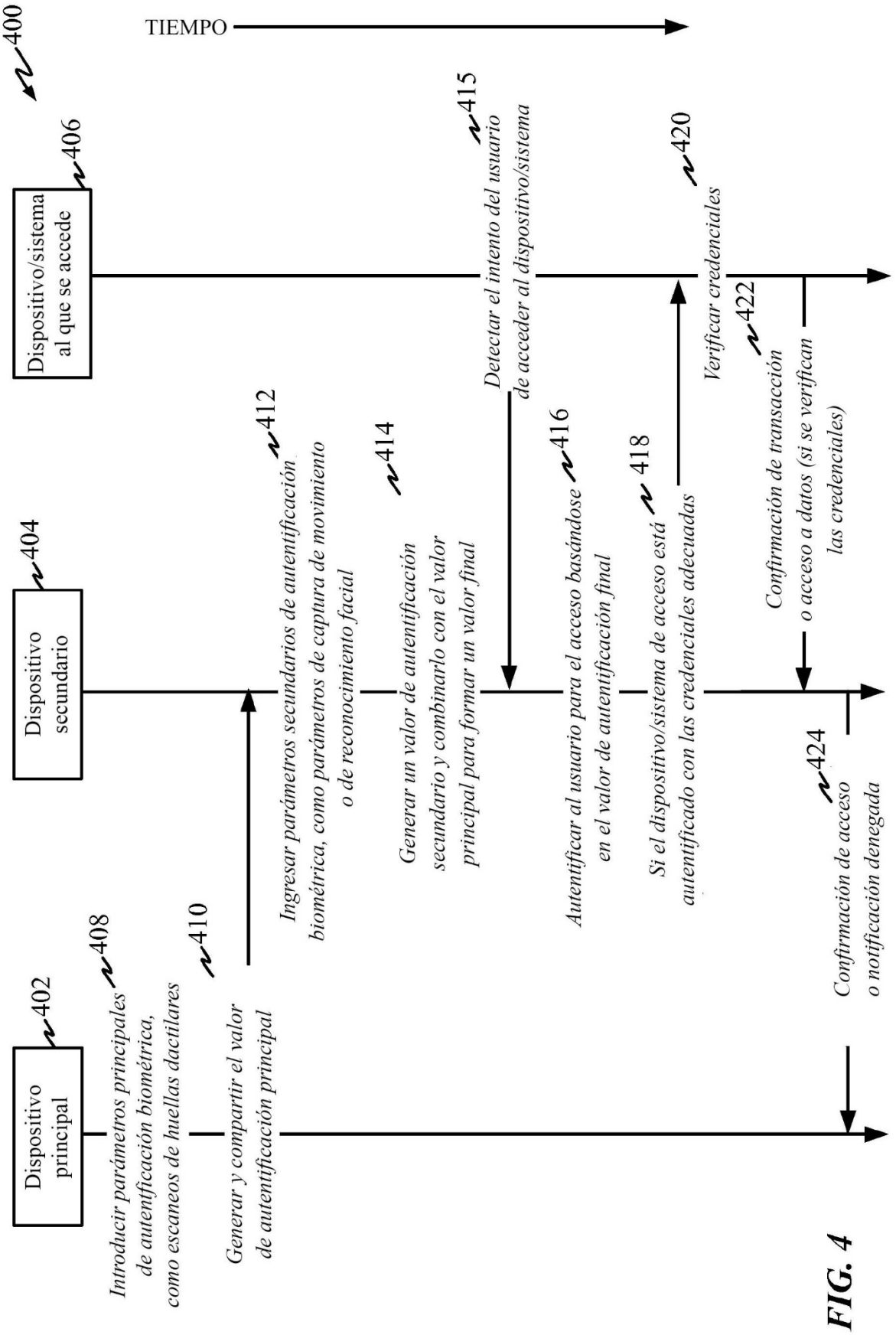
400
TIEMPO
Dispositivo principal
402
Dispositivo secundario
404
Dispositivo/sistema al que se accede
406
Introducir parámetros principales de autentificación biométrica, como escaneos de huellas dactilares
408
Generar y compartir el valor de autentificación principal
410
Ingresar parámetros secundarios de autentificación biométrica, como parámetros de captura de movimiento o de reconocimiento facial
412
Generar un valor de autentificación secundario y combinarlo con el valor principal para formar un valor final
414
Detectar el intento del usuario de acceder al dispositivo/sistema
415
Autentificar al usuario para el acceso basándose en el valor de autentificación final
416
Si el dispositivo/sistema de acceso está autentificado con las credenciales adecuadas
418
Verificar credenciales
420
Confirmación de transacción o acceso a datos (si se verifican las credenciales)
422
Confirmación de acceso o notificación denegada
424

FIG. 4

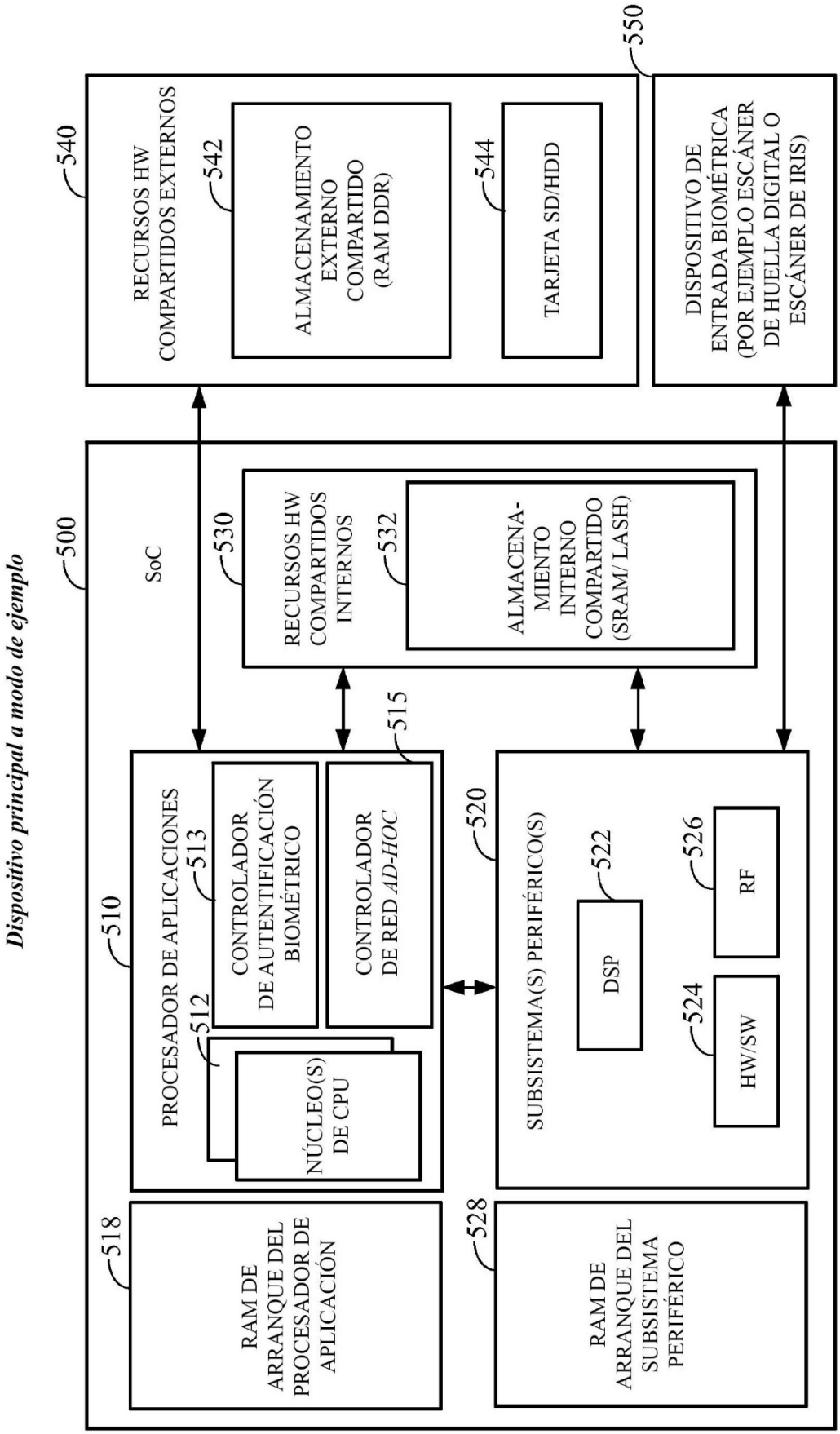
Dispositivo principal a modo de ejemplo
500
SoC
510
PROCESADOR DE APLICACIONES
512
NÚCLEO(S) DE CPU
513
CONTROLADOR DE AUTENTIFICACIÓN BIOMÉTRICO
515
CONTROLADOR DE RED AD-HOC
518
RAM DE ARRANQUE DEL PROCESADOR DE APLICACIÓN
520
SUBSISTEMA(S) PERIFÉRICO(S)
522
DSP
524
HW/SW
526
RF
528
RAM DE ARRANQUE DEL SUBSISTEMA PERIFÉRICO
530
RECURSOS HW COMPARTIDOS INTERNOS
532
ALMACENA-MIENTO INTERNO COMPARTIDO (SRAM/ LASH)
540
RECURSOS HW COMPARTIDOS EXTERNOS
542
ALMACENAMIENTO EXTERNO COMPARTIDO (RAM DDR)
544
TARJETA SD/HDD
550
DISPOSITIVO DE ENTRADA BIOMÉTRICA (POR EJEMPLO ESCÁNER DE HUELLA DIGITAL O ESCÁNER DE IRIS)

FIG. 5

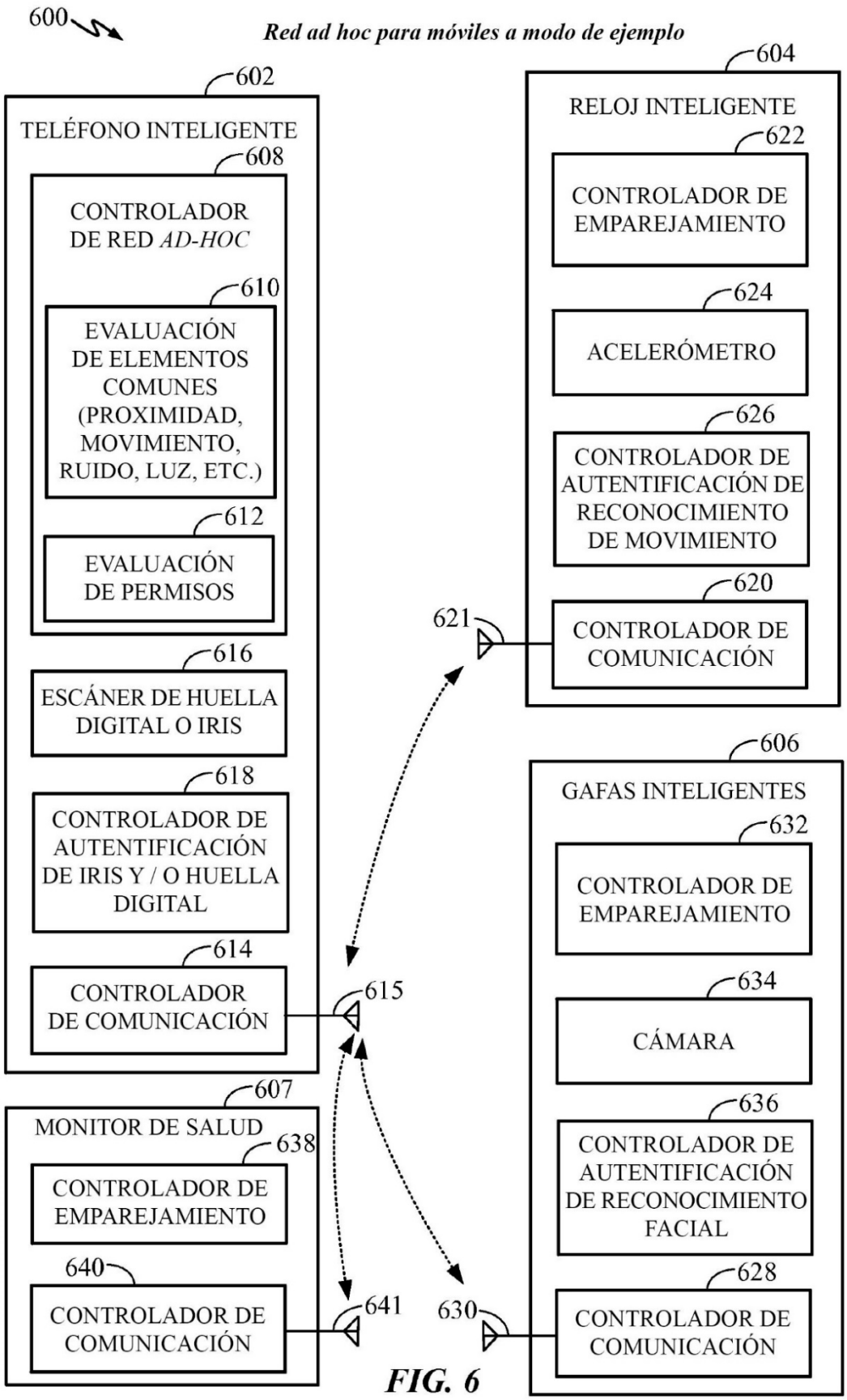
600
Red ad hoc para móviles a modo de ejemplo
602
TELÉFONO INTELIGENTE
608
CONTROLADOR DE RED AD-HOC
610
EVALUACIÓN DE ELEMENTOS COMUNES (PROXIMIDAD, MOVIMIENTO, RUIDO, LUZ, ETC.)
612
EVALUACIÓN DE PERMISOS
616
ESCÁNER DE HUELLA DIGITAL O IRIS
618
CONTROLADOR DE AUTENTIFICACIÓN DE IRIS Y / O HUELLA DIGITAL
614
CONTROLADOR DE COMUNICACIÓN
615
607
MONITOR DE SALUD
638
CONTROLADOR DE EMPAREJAMIENTO
640
CONTROLADOR DE COMUNICACIÓN
641
604
RELOJ INTELIGENTE
622
CONTROLADOR DE EMPAREJAMIENTO
624
ACELERÓMETRO
626
CONTROLADOR DE AUTENTIFICACIÓN DE RECONOCIMIENTO DE MOVIMIENTO
620
621
CONTROLADOR DE COMUNICACIÓN
606
GAFAS INTELIGENTES
632
CONTROLADOR DE EMPAREJAMIENTO
634
CÁMARA
636
CONTROLADOR DE AUTENTIFICACIÓN DE RECONOCIMIENTO FACIAL
628
630
CONTROLADOR DE COMUNICACIÓN

FIG. 6

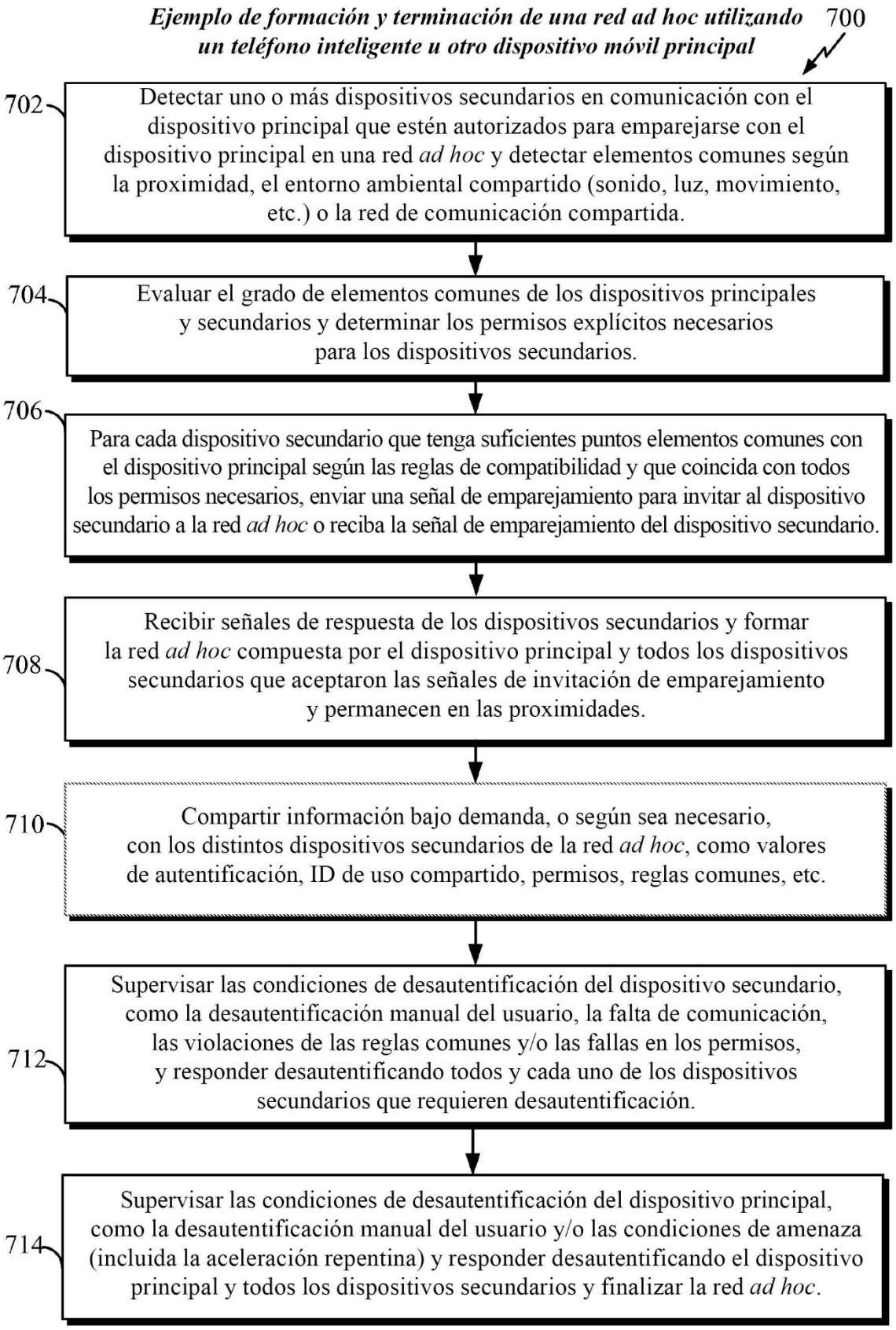
Ejemplo de formación y terminación de una red ad hoc utilizando un teléfono inteligente u otro dispositivo móvil principal
700
702
Detectar uno o más dispositivos secundarios en comunicación con el dispositivo principal que estén autorizados para emparejarse con el dispositivo principal en una red ad hoc y detectar elementos comunes según la proximidad, el entorno ambiental compartido (sonido, luz, movimiento, etc.) o la red de comunicación compartida.
704
Evaluar el grado de elementos comunes de los dispositivos principales y secundarios y determinar los permisos explícitos necesarios para los dispositivos secundarios.
706
Para cada dispositivo secundario que tenga suficientes puntos elementos comunes con el dispositivo principal según las reglas de compatibilidad y que coincida con todos los permisos necesarios, enviar una señal de emparejamiento para invitar al dispositivo secundario a la red ad hoc o reciba la señal de emparejamiento del dispositivo secundario.
708
Recibir señales de respuesta de los dispositivos secundarios y formar la red ad hoc compuesta por el dispositivo principal y todos los dispositivos secundarios que aceptaron las señales de invitación de emparejamiento y permanecen en las proximidades.
710
Compartir información bajo demanda, o según sea necesario, con los distintos dispositivos secundarios de la red ad hoc, como valores de autentificación, ID de uso compartido, permisos, reglas comunes, etc.
712
Supervisar las condiciones de desautentificación del dispositivo secundario, como la desautentificación manual del usuario, la falta de comunicación, las violaciones de las reglas comunes y/o las fallas en los permisos, y responder desautentificando todos y cada uno de los dispositivos secundarios que requieren desautentificación.
714
Supervisar las condiciones de desautentificación del dispositivo principal, como la desautentificación manual del usuario y/o las condiciones de amenaza (incluida la aceleración repentina) y responder desautentificando el dispositivo principal y todos los dispositivos secundarios y finalizar la red ad hoc.

FIG. 7

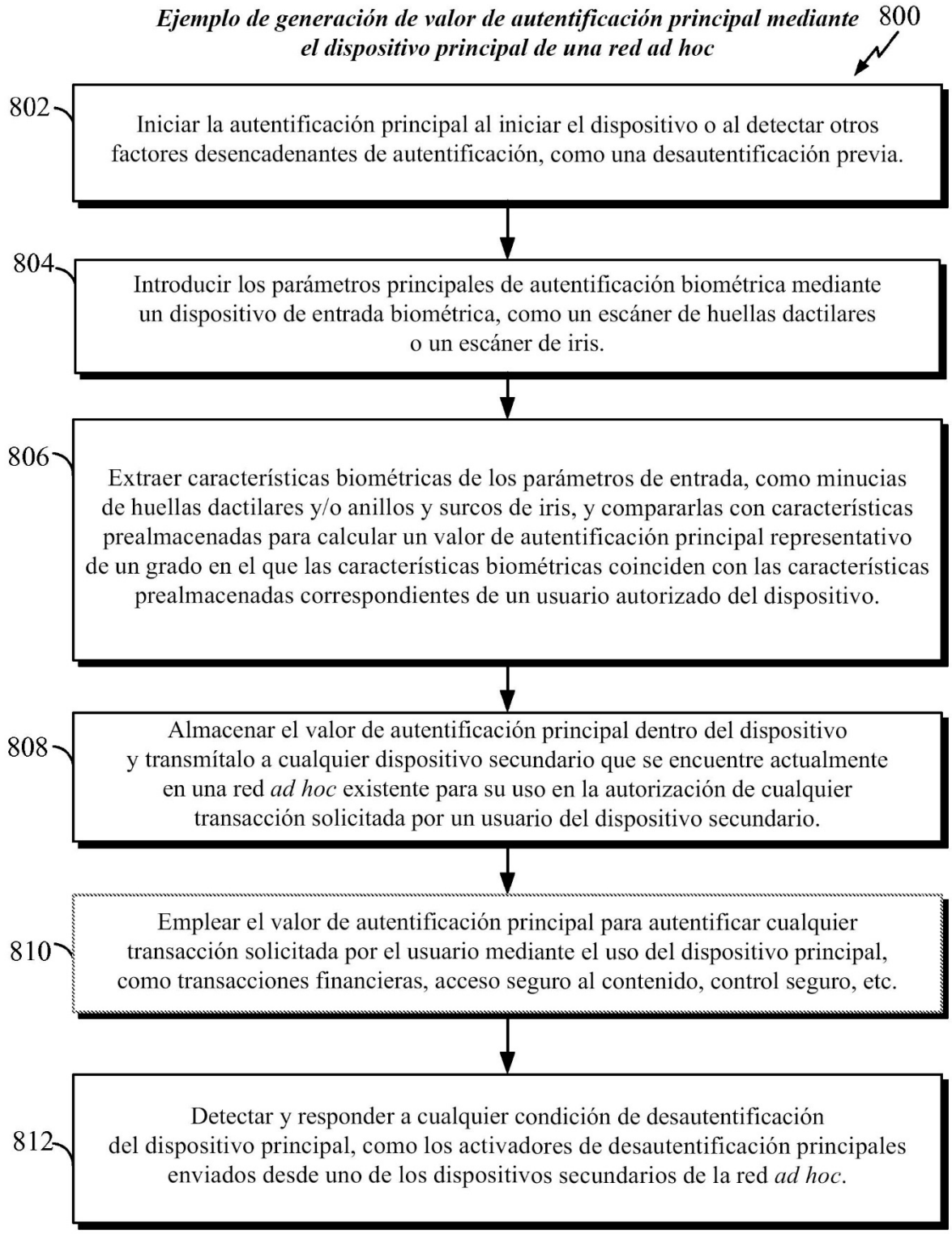
Ejemplo de generación de valor de autentificación principal mediante el dispositivo principal de una red ad hoc
800
802
Iniciar la autentificación principal al iniciar el dispositivo o al detectar otros factores desencadenantes de autentificación, como una desautentificación previa.
804
Introducir los parámetros principales de autentificación biométrica mediante un dispositivo de entrada biométrica, como un escáner de huellas dactilares o un escáner de iris.
806
Extraer características biométricas de los parámetros de entrada, como minucias de huellas dactilares y/o anillos y surcos de iris, y compararlas con características prealmacenadas para calcular un valor de autentificación principal representativo de un grado en el que las características biométricas coinciden con las características prealmacenadas correspondientes de un usuario autorizado del dispositivo.
808
Almacenar el valor de autentificación principal dentro del dispositivo y transmítalo a cualquier dispositivo secundario que se encuentre actualmente en una red ad hoc existente para su uso en la autorización de cualquier transacción solicitada por un usuario del dispositivo secundario.
810
Emplear el valor de autentificación principal para autentificar cualquier transacción solicitada por el usuario mediante el uso del dispositivo principal, como transacciones financieras, acceso seguro al contenido, control seguro, etc.
812
Detectar y responder a cualquier condición de desautentificación del dispositivo principal, como los activadores de desautentificación principales enviados desde uno de los dispositivos secundarios de la red ad hoc.

FIG. 8

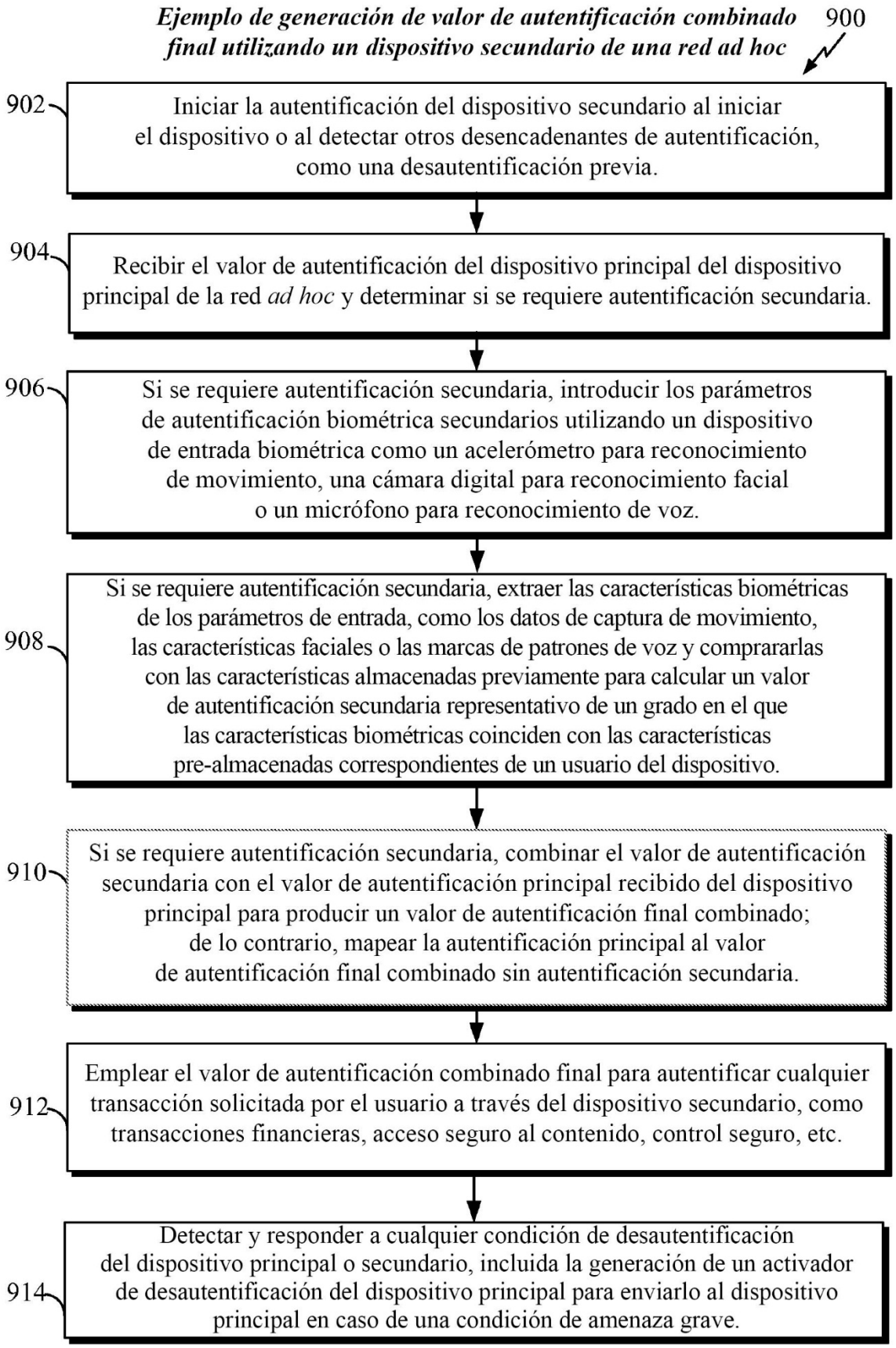
Ejemplo de generación de valor de autentificación combinado final utilizando un dispositivo secundario de una red ad hoc
900
902
Iniciar la autentificación del dispositivo secundario al iniciar el dispositivo o al detectar otros desencadenantes de autentificación, como una desautentificación previa.
904
Recibir el valor de autentificación del dispositivo principal del dispositivo principal de la red ad hoc y determinar si se requiere autentificación secundaria.
906
Si se requiere autentificación secundaria, introducir los parámetros de autentificación biométrica secundarios utilizando un dispositivo de entrada biométrica como un acelerómetro para reconocimiento de movimiento, una cámara digital para reconocimiento facial o un micrófono para reconocimiento de voz.
908
Si se requiere autentificación secundaria, extraer las características biométricas de los parámetros de entrada, como los datos de captura de movimiento, las características faciales o las marcas de patrones de voz y compararlas con las características almacenadas previamente para calcular un valor de autentificación secundaria representativo de un grado en el que las características biométricas coinciden con las características pre-almacenadas correspondientes de un usuario del dispositivo.
910
Si se requiere autentificación secundaria, combinar el valor de autentificación secundaria con el valor de autentificación principal recibido del dispositivo principal para producir un valor de autentificación final combinado; de lo contrario, mapear la autentificación principal al valor de autentificación final combinado sin autentificación secundaria.
912
Emplear el valor de autentificación combinado final para autentificar cualquier transacción solicitada por el usuario a través del dispositivo secundario, como transacciones financieras, acceso seguro al contenido, control seguro, etc.
914
Detectar y responder a cualquier condición de desautentificación del dispositivo principal o secundario, incluida la generación de un activador de desautentificación del dispositivo principal para enviarlo al dispositivo principal en caso de una condición de amenaza grave.

FIG. 9

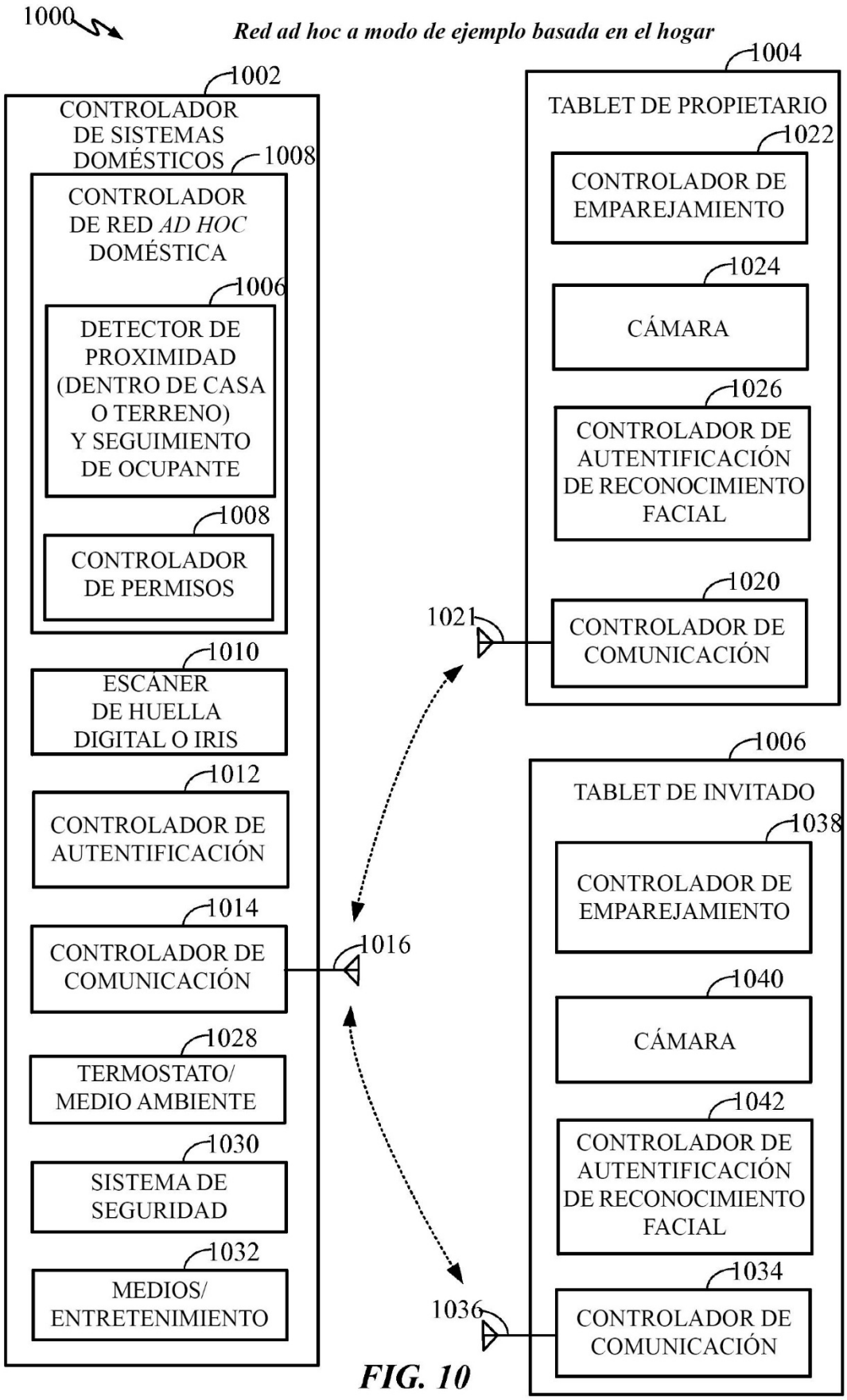
1000
Red ad hoc a modo de ejemplo basada en el hogar
1002
CONTROLADOR DE SISTEMAS DOMÉSTICOS
1008
CONTROLADOR DE RED AD HOC DOMÉSTICA
1006
DETECTOR DE PROXIMIDAD (DENTRO DE CASA O TERRENO) Y SEGUIMIENTO DE OCUPANTE
1008
CONTROLADOR DE PERMISOS
1010
ESCÁNER DE HUELLA DIGITAL O IRIS
1012
CONTROLADOR DE AUTENTIFICACIÓN
1014
CONTROLADOR DE COMUNICACIÓN
1028
TERMOSTATO/ MEDIO AMBIENTE
1030
SISTEMA DE SEGURIDAD
1032
MEDIOS/ ENTRETENIMIENTO
1016
1004
TABLET DE PROPIETARIO
1022
CONTROLADOR DE EMPAREJAMIENTO
1024
CÁMARA
1026
CONTROLADOR DE AUTENTIFICACIÓN DE RECONOCIMIENTO FACIAL
1020
1021
CONTROLADOR DE COMUNICACIÓN
1006
TABLET DE INVITADO
1038
CONTROLADOR DE EMPAREJAMIENTO
1040
CÁMARA
1042
CONTROLADOR DE AUTENTIFICACIÓN DE RECONOCIMIENTO FACIAL
1034
1036
CONTROLADOR DE COMUNICACIÓN

FIG. 10

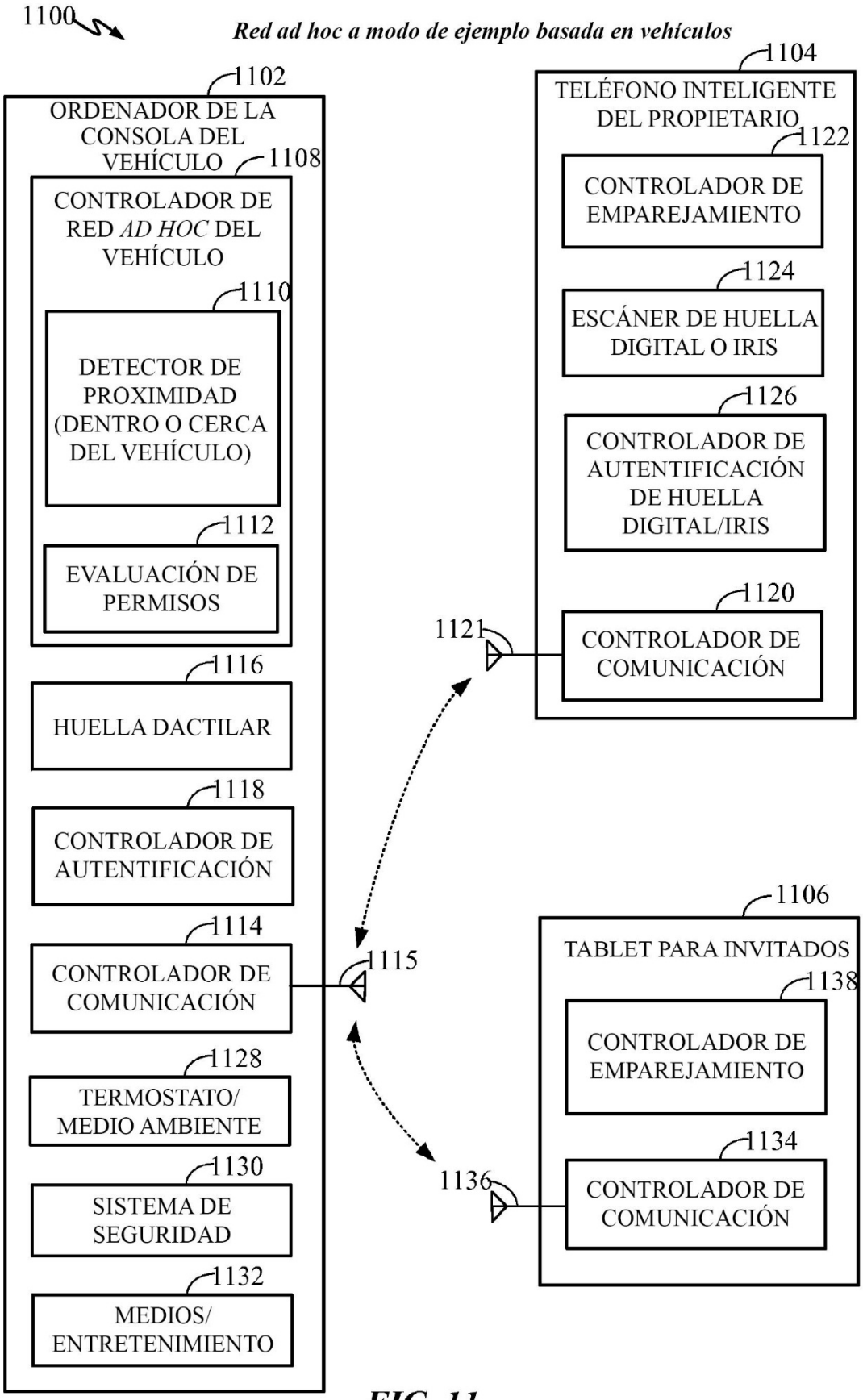
1100
Red ad hoc a modo de ejemplo basada en vehículos
1102
ORDENADOR DE LA CONSOLA DEL VEHÍCULO
1108
CONTROLADOR DE RED AD HOC DEL VEHÍCULO
1110
DETECTOR DE PROXIMIDAD (DENTRO O CERCA DEL VEHÍCULO)
1112
EVALUACIÓN DE PERMISOS
1116
HUELLA DACTILAR
1118
CONTROLADOR DE AUTENTIFICACIÓN
1114
CONTROLADOR DE COMUNICACIÓN
1128
TERMOSTATO/ MEDIO AMBIENTE
1130
SISTEMA DE SEGURIDAD
1132
MEDIOS/ ENTRETENIMIENTO
1115
1104
TELÉFONO INTELIGENTE DEL PROPIETARIO
1122
CONTROLADOR DE EMPAREJAMIENTO
1124
ESCÁNER DE HUELLA DIGITAL O IRIS
1126
CONTROLADOR DE AUTENTIFICACIÓN DE HUELLA DIGITAL/IRIS
1120
1121
CONTROLADOR DE COMUNICACIÓN
1106
TABLET PARA INVITADOS
1138
CONTROLADOR DE EMPAREJAMIENTO
1134
1136
CONTROLADOR DE COMUNICACIÓN

FIG. 11

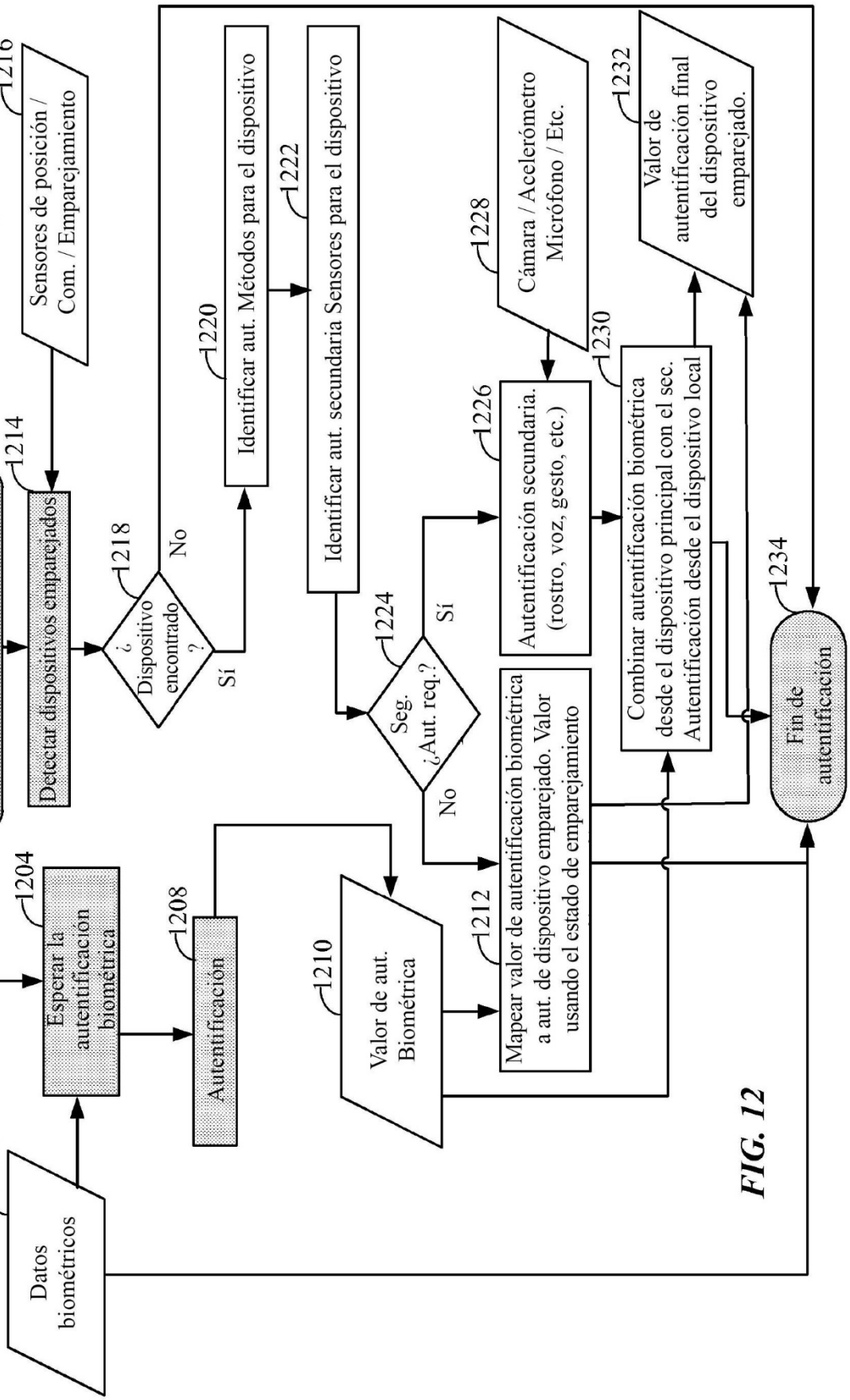
1200
Inicio de autentificación
1202
Detectar dispositivos emparejados
1214
Sensores de posición / Com. / Emparejamiento
1216
¿ Dispositivo encontrado ?
1218
No
Sí
Identificar aut. Métodos para el dispositivo
1220
Identificar aut. secundaria Sensores para el dispositivo
1222
Seg. ¿Aut. req.?
1224
Sí
No
Autentificación secundaria. (rostro, voz, gesto, etc.)
1226
Cámara / Acelerómetro Micrófono / Etc.
1228
Combinar autentificación biométrica desde el dispositivo principal con el sec. Autentificación desde el dispositivo local
1230
Valor de autentificación final del dispositivo emparejado.
1232
Fin de autentificación
1234
Esperar la autentificación biométrica
1204
Autentificación
1208
Datos biométricos
1206
Valor de aut. Biométrica
1210
Mapear valor de autentificación biométrica a aut. de dispositivo emparejado. Valor usando el estado de emparejamiento
1212

FIG. 12

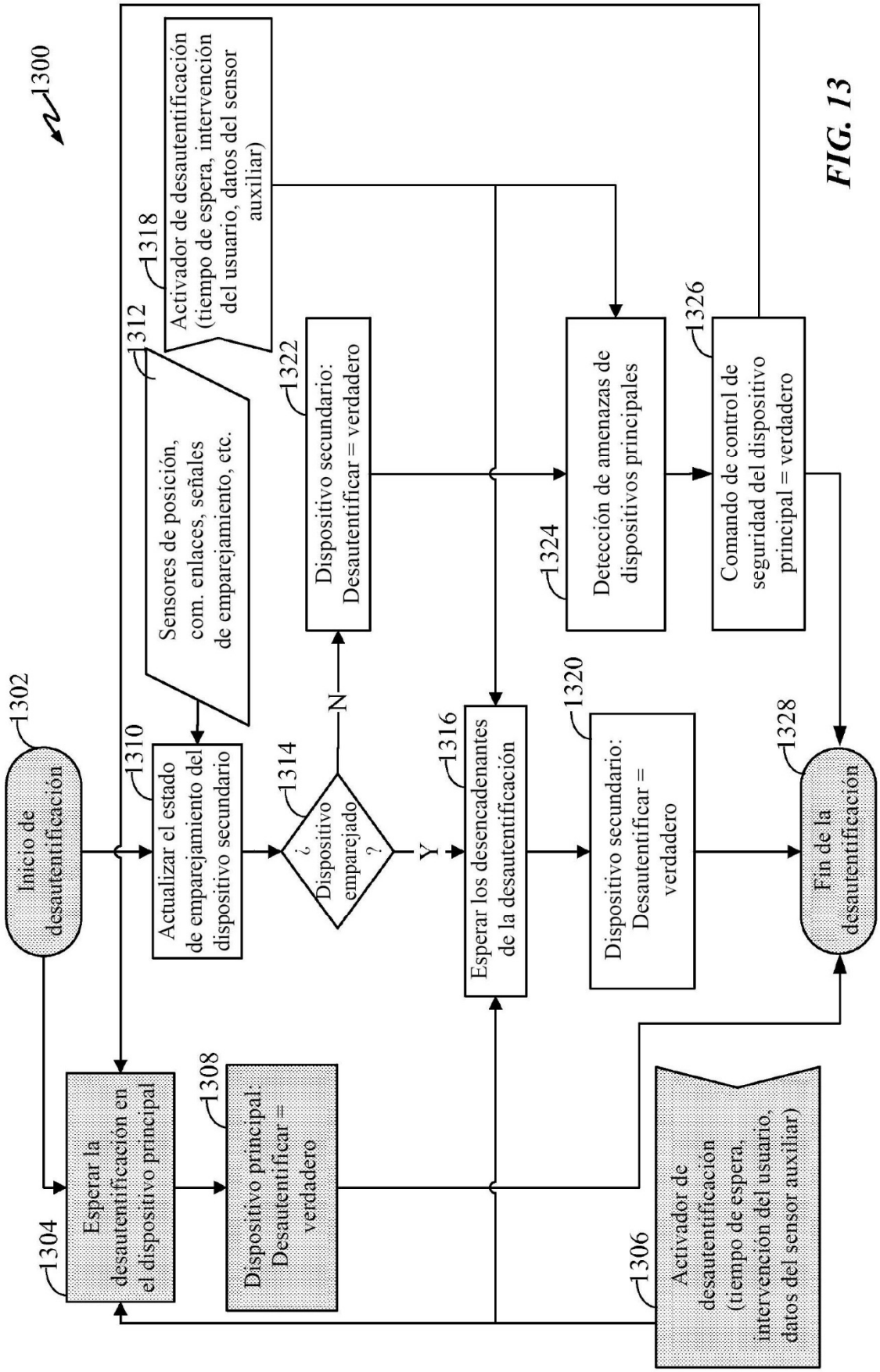
1300
1302
Inicio de desautentificación
1304
Esperar la desautentificación en el dispositivo principal
1306
Activador de desautentificación (tiempo de espera, intervención del usuario, datos del sensor auxiliar)
1308
Dispositivo principal: Desautentificar = verdadero
1310
Actualizar el estado de emparejamiento del dispositivo secundario
1312
Sensores de posición, com. enlaces, señales de emparejamiento, etc.
1314
¿Dispositivo emparejado?
Y
N
1316
Esperar los desencadenantes de la desautentificación
1318
Activador de desautentificación (tiempo de espera, intervención del usuario, datos del sensor auxiliar)
1320
Dispositivo secundario: Desautentificar = verdadero
1322
Dispositivo secundario: Desautentificar = verdadero
1324
Detección de amenazas de dispositivos principales
1326
Comando de control de seguridad del dispositivo principal = verdadero
1328
Fin de la desautentificación

FIG. 13

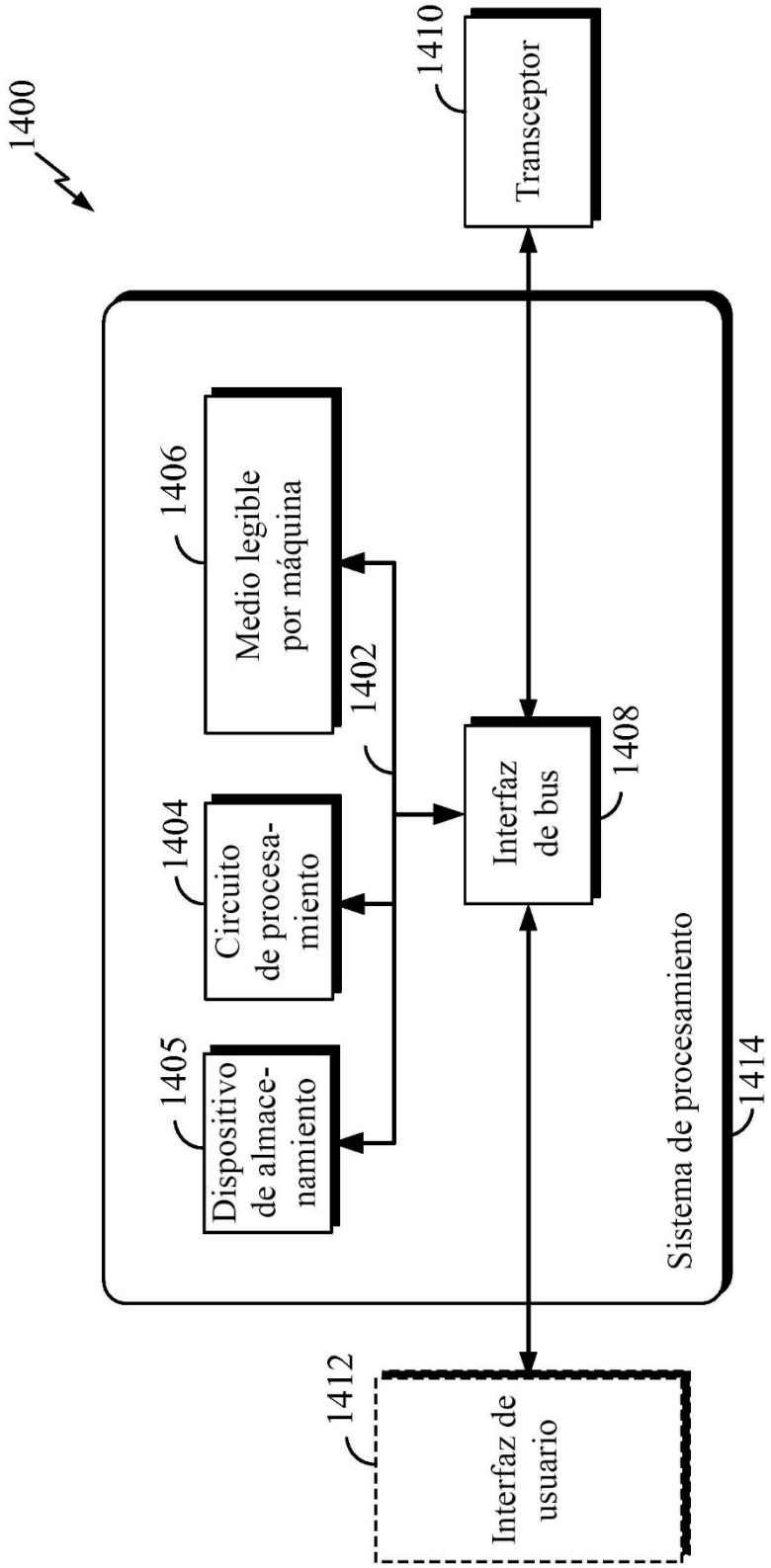
1400
1410
Transceptor
1406
Medio legible por máquina
1402
1404
Circuito de procesa-miento
1408
Interfaz de bus
1405
Dispositivo de almace-namiento
Sistema de procesamiento
1414
1412
Interfaz de usuario

FIG. 14

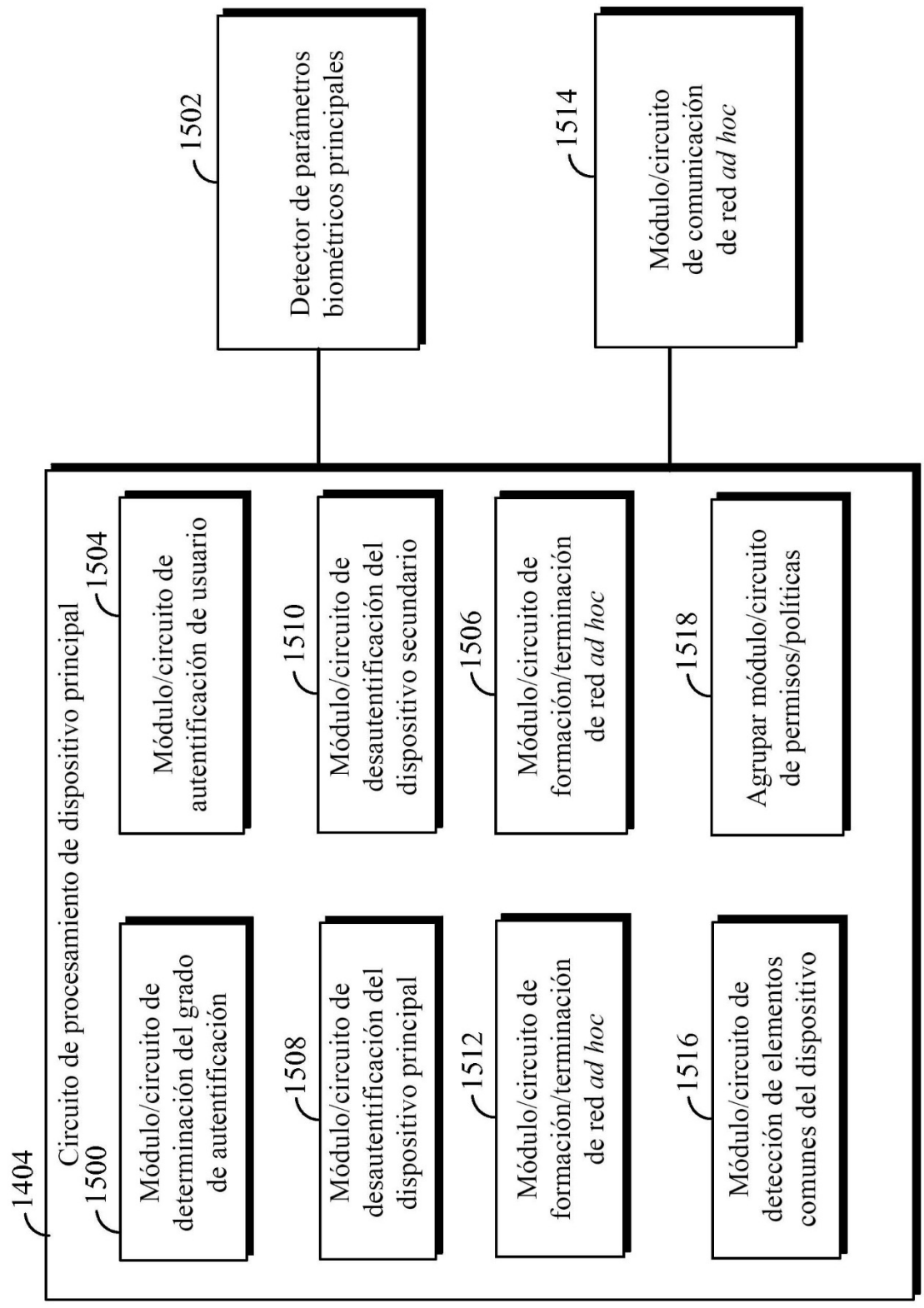
1404
Circuito de procesamiento de dispositivo principal
1500
Módulo/circuito de determinación del grado de autentificación
1504
Módulo/circuito de autentificación de usuario
1508
Módulo/circuito de desautentificación del dispositivo principal
1510
Módulo/circuito de desautentificación del dispositivo secundario
1512
Módulo/circuito de formación/terminación de red *ad hoc*
1506
Módulo/circuito de formación/terminación de red *ad hoc*
1516
Módulo/circuito de detección de elementos comunes del dispositivo
1518
Agrupar módulo/circuito de permisos/políticas
1502
Detector de parámetros biométricos principales
1514
Módulo/circuito de comunicación de red *ad hoc*

FIG. 15

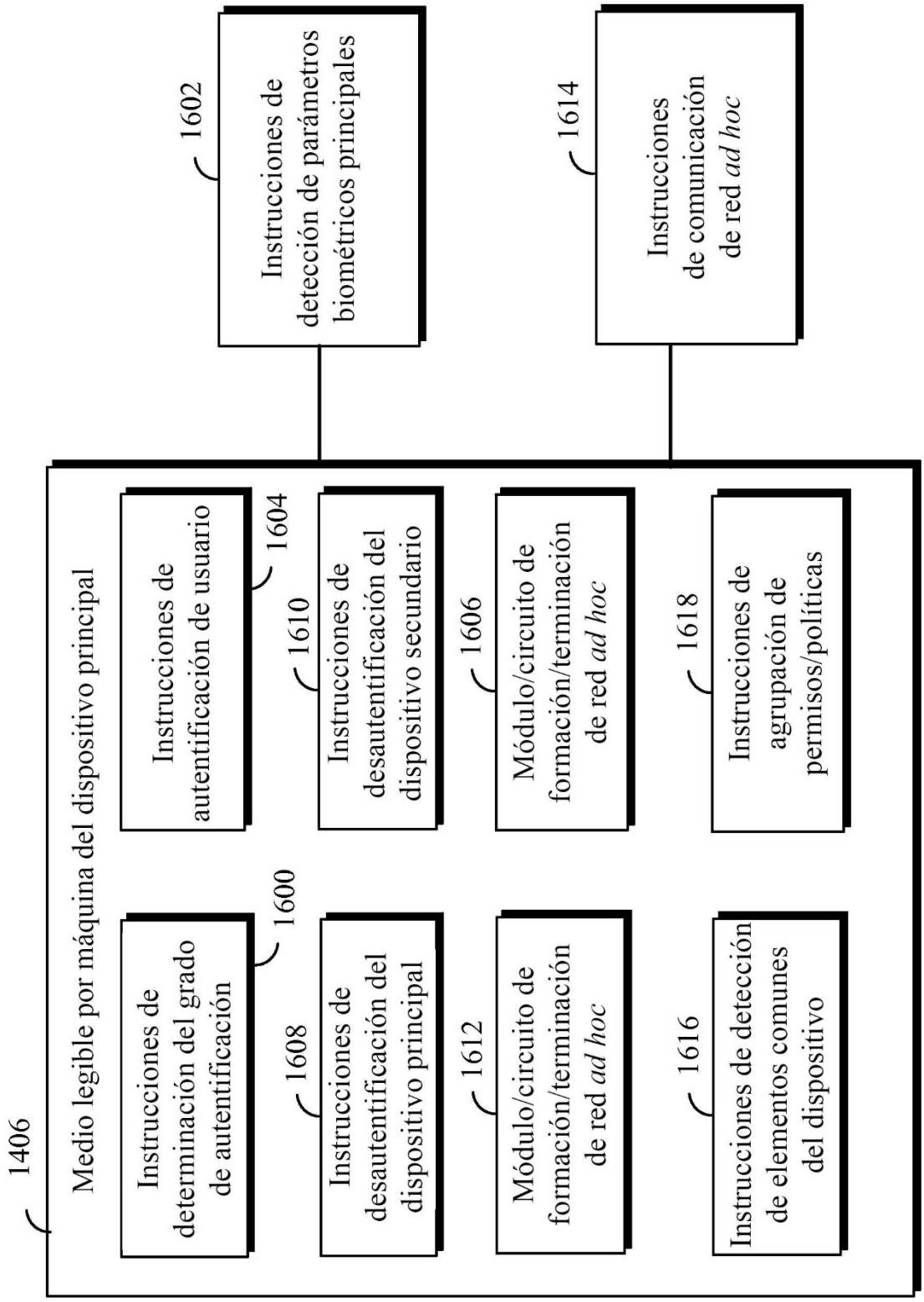
1406
Medio legible por máquina del dispositivo principal
1600
Instrucciones de determinación del grado de autentificación
1608
Instrucciones de desautentificación del dispositivo principal
1612
Módulo/circuito de formación/terminación de red *ad hoc*
1616
Instrucciones de detección de elementos comunes del dispositivo
1604
Instrucciones de autentificación de usuario
1610
Instrucciones de desautentificación del dispositivo secundario
1606
Módulo/circuito de formación/terminación de red *ad hoc*
1618
Instrucciones de agrupación de permisos/políticas
1602
Instrucciones de detección de parámetros biométricos principales
1614
Instrucciones de comunicación de red *ad hoc*

FIG. 16

Resumen del método que debe utilizar un dispositivo principal de una red ad hoc para la autentificación de un usuario

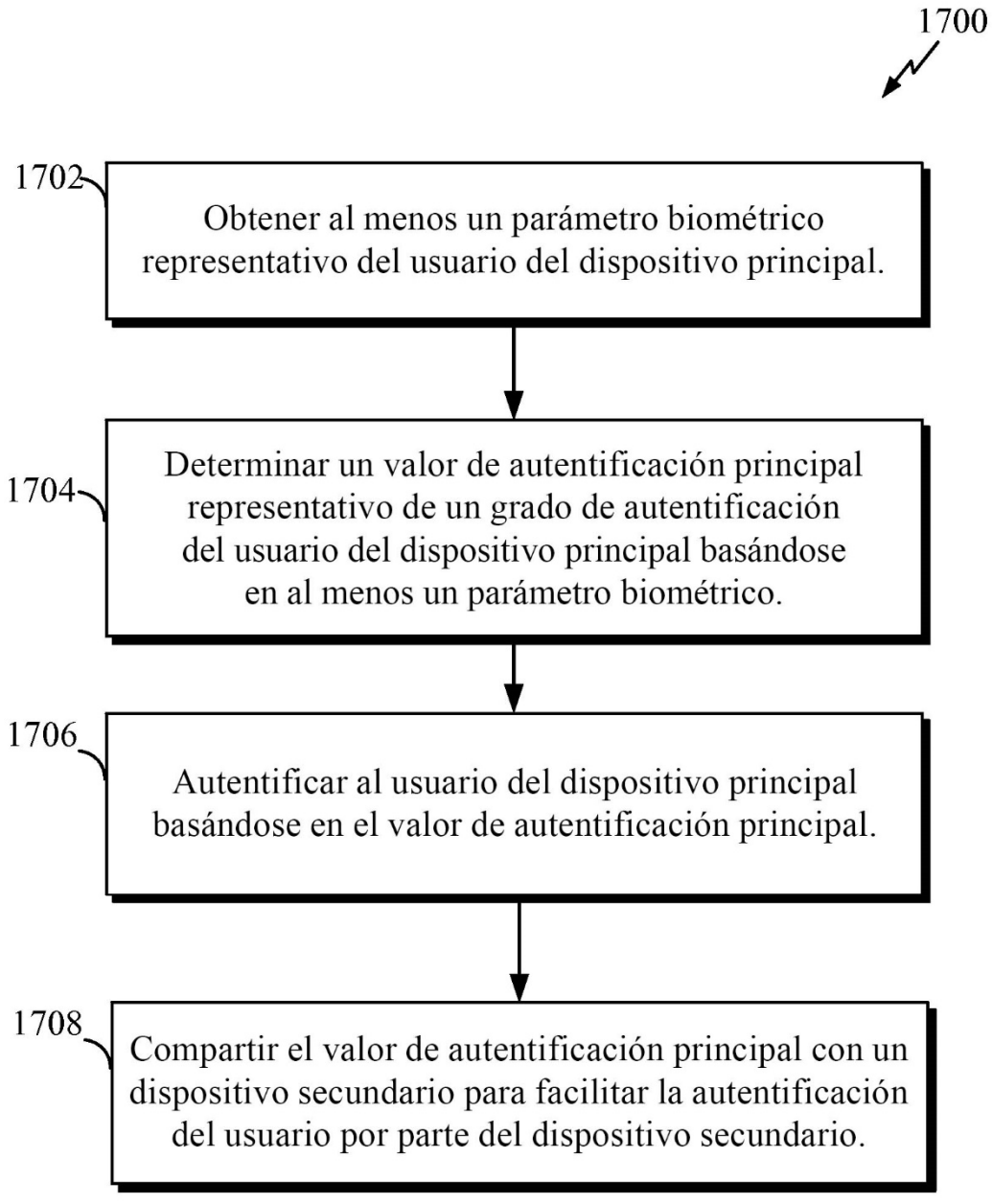

FIG. 17

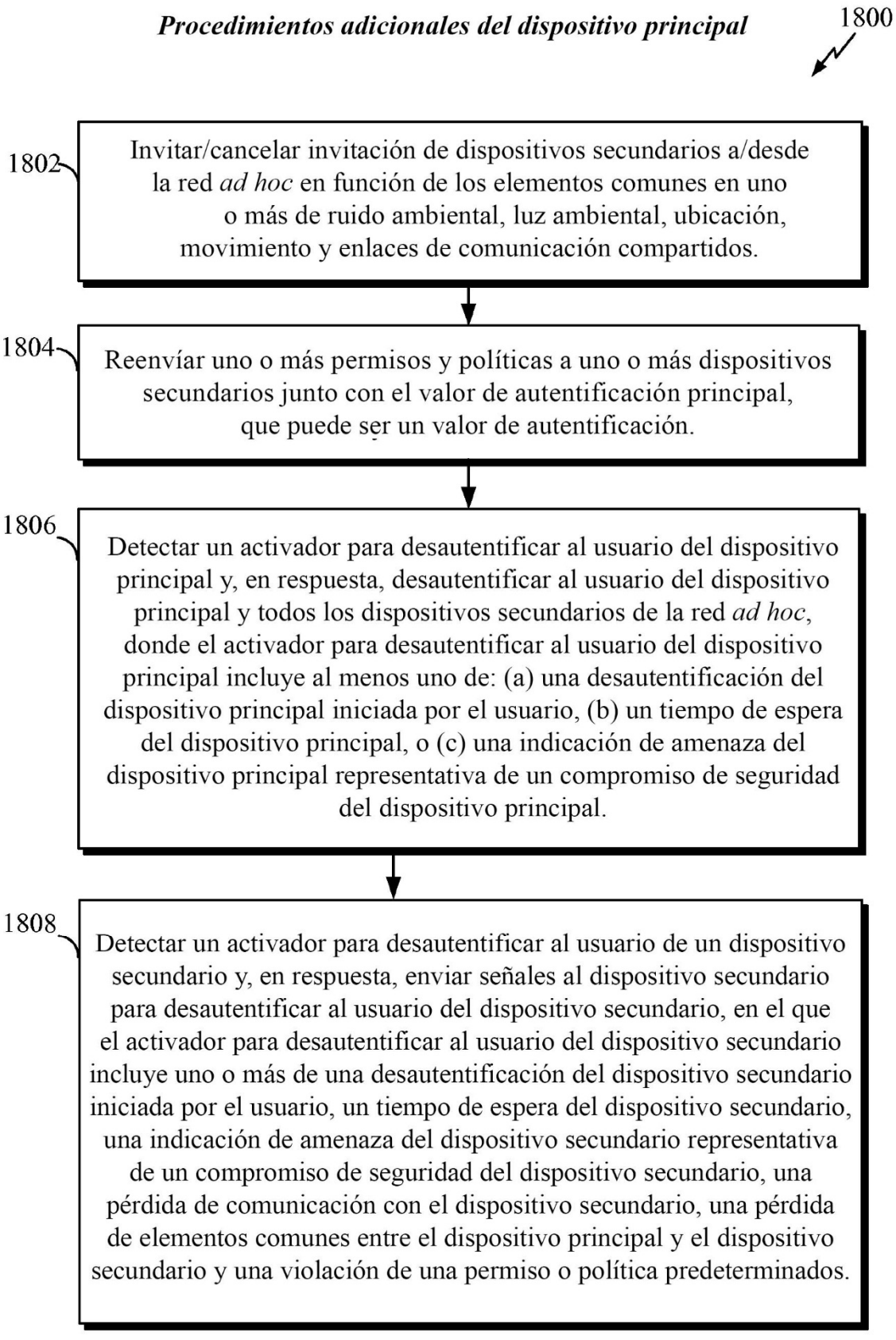
Procedimientos adicionales del dispositivo principal
1800
1802
Invitar/cancelar invitación de dispositivos secundarios a/desde la red *ad hoc* en función de los elementos comunes en uno o más de ruido ambiental, luz ambiental, ubicación, movimiento y enlaces de comunicación compartidos.
1804
Reenvíar uno o más permisos y políticas a uno o más dispositivos secundarios junto con el valor de autentificación principal, que puede ser un valor de autentificación.
1806
Detectar un activador para desautentificar al usuario del dispositivo principal y, en respuesta, desautentificar al usuario del dispositivo principal y todos los dispositivos secundarios de la red *ad hoc*, donde el activador para desautentificar al usuario del dispositivo principal incluye al menos uno de: (a) una desautentificación del dispositivo principal iniciada por el usuario, (b) un tiempo de espera del dispositivo principal, o (c) una indicación de amenaza del dispositivo principal representativa de un compromiso de seguridad del dispositivo principal.
1808
Detectar un activador para desautentificar al usuario de un dispositivo secundario y, en respuesta, enviar señales al dispositivo secundario para desautentificar al usuario del dispositivo secundario, en el que el activador para desautentificar al usuario del dispositivo secundario incluye uno o más de una desautentificación del dispositivo secundario iniciada por el usuario, un tiempo de espera del dispositivo secundario, una indicación de amenaza del dispositivo secundario representativa de un compromiso de seguridad del dispositivo secundario, una pérdida de comunicación con el dispositivo secundario, una pérdida de elementos comunes entre el dispositivo principal y el dispositivo secundario y una violación de una permiso o política predeterminados.

FIG. 18

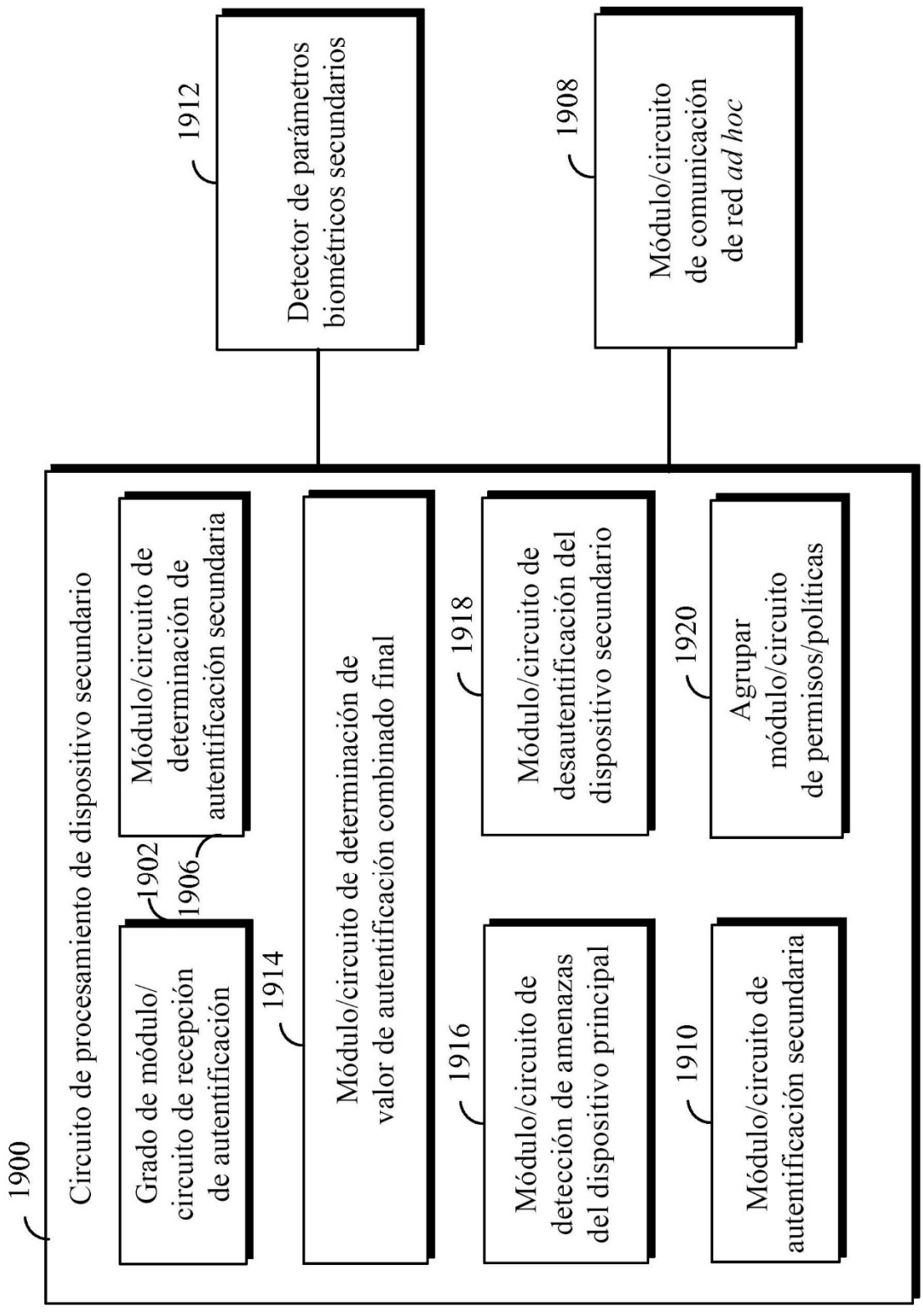
1900
Circuito de procesamiento de dispositivo secundario
Grado de módulo/ circuito de recepción de autentificación
1902
1906
Módulo/circuito de determinación de autentificación secundaria
1914
Módulo/circuito de determinación de valor de autentificación combinado final
1916
Módulo/circuito de detección de amenazas del dispositivo principal
1910
Módulo/circuito de autentificación secundaria
1918
Módulo/circuito de desautentificación del dispositivo secundario
1920
Agrupar módulo/circuito de permisos/políticas
1912
Detector de parámetros biométricos secundarios
1908
Módulo/circuito de comunicación de red *ad hoc*

FIG. 19

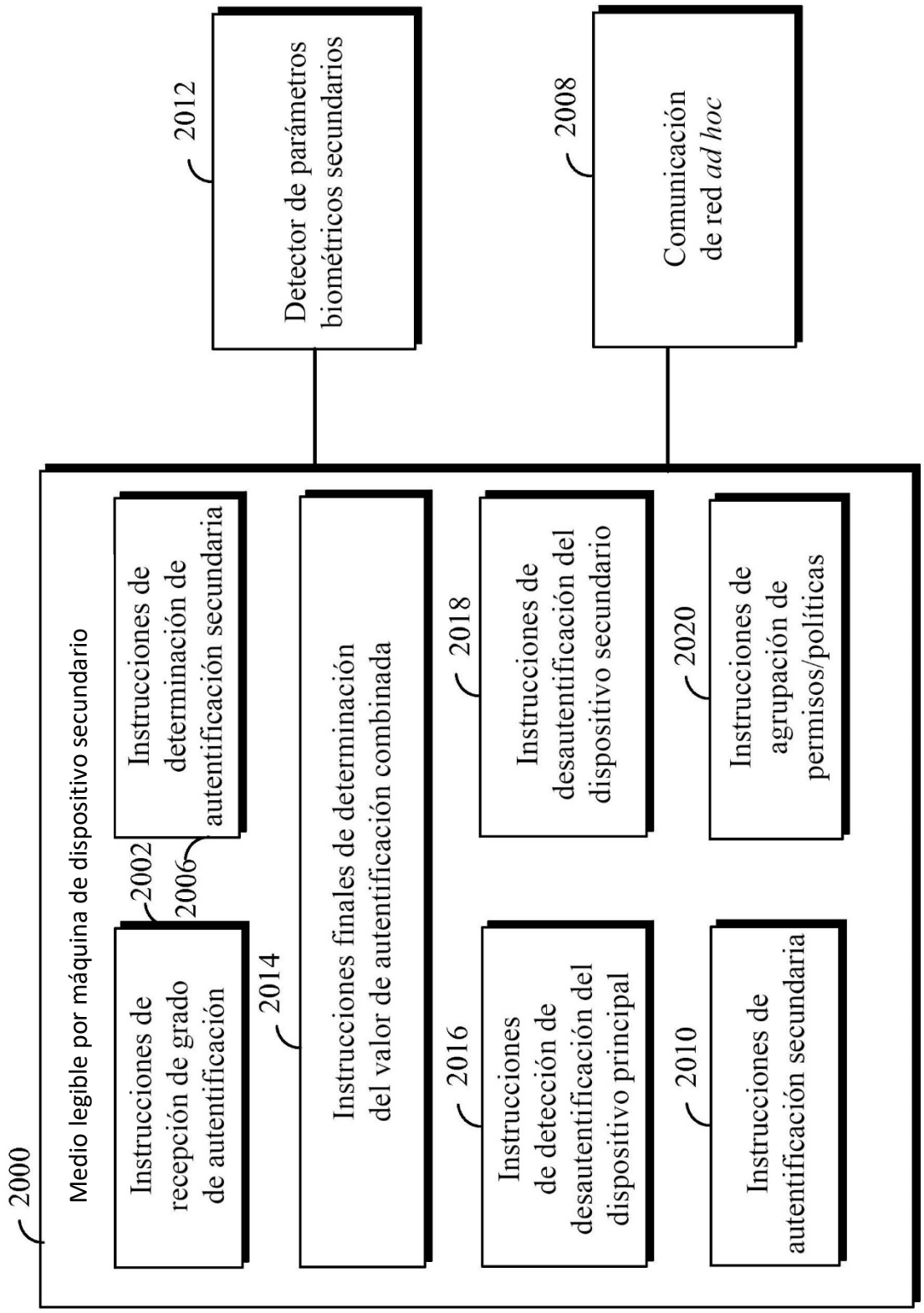
2000
Medio legible por máquina de dispositivo secundario
Instrucciones de recepción de grado de autentificación
2002
2006
Instrucciones de determinación de autentificación secundaria
2014
Instrucciones finales de determinación del valor de autentificación combinada
2016
Instrucciones de detección de desautentificación del dispositivo principal
2018
Instrucciones de desautentificación del dispositivo secundario
2010
Instrucciones de autentificación secundaria
2020
Instrucciones de agrupación de permisos/políticas
2012
Detector de parámetros biométricos secundarios
2008
Comunicación de red *ad hoc*

FIG. 20

Resumen del procedimiento que debe utilizar un dispositivo secundario de una red ad hoc para la autentificación de un usuario

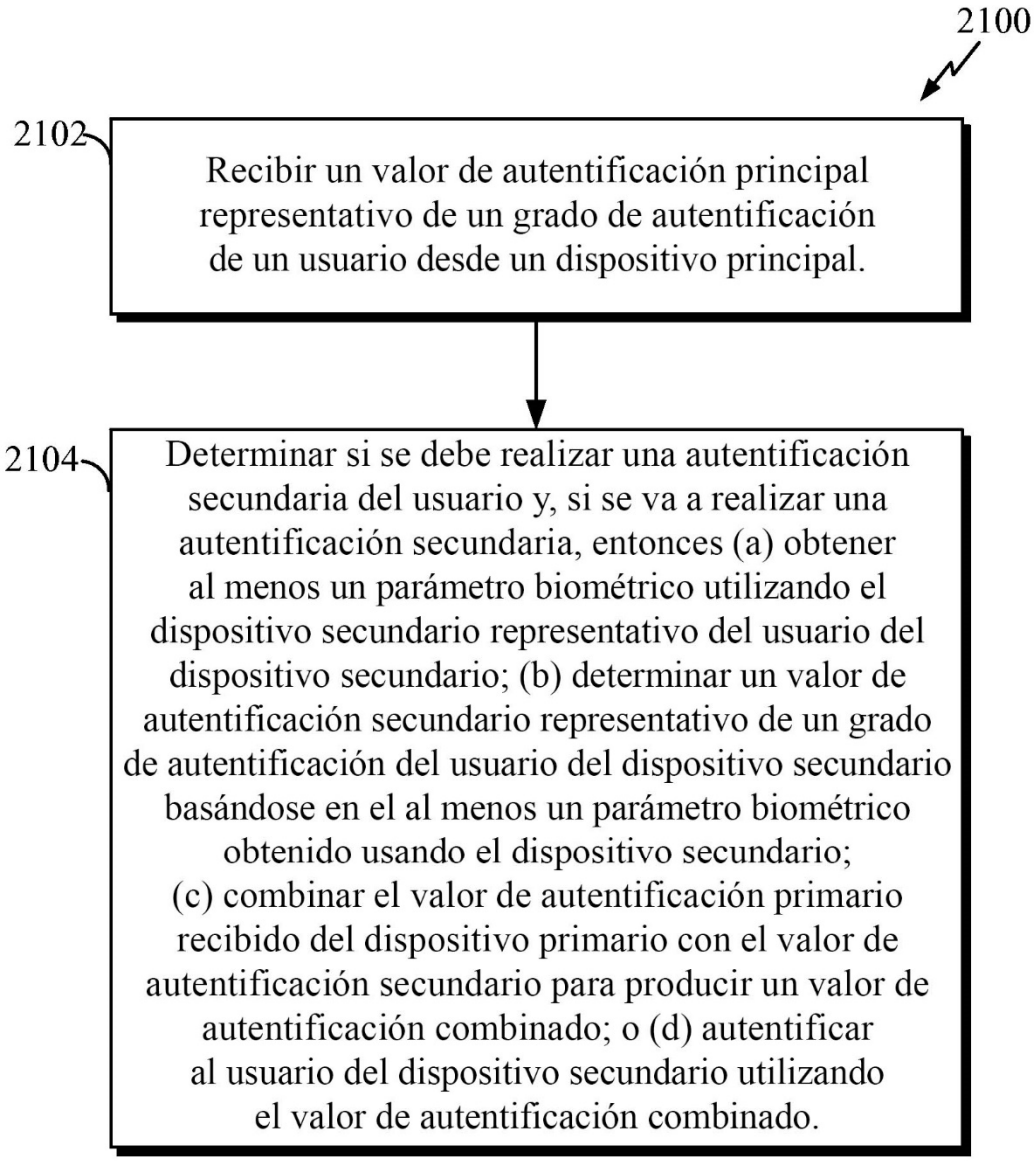

FIG. 21

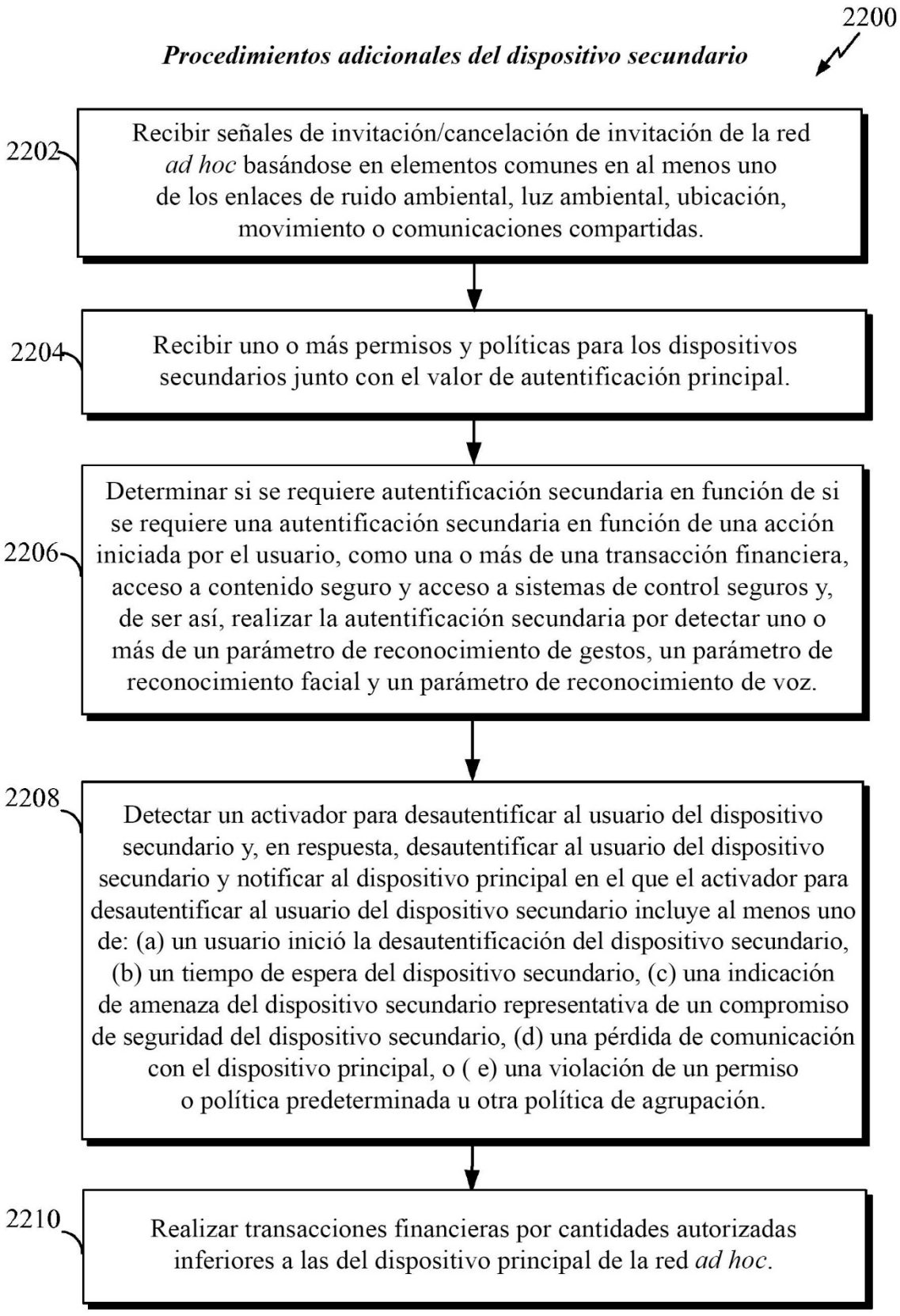
2200
Procedimientos adicionales del dispositivo secundario
2202
Recibir señales de invitación/cancelación de invitación de la red ad hoc basándose en elementos comunes en al menos uno de los enlaces de ruido ambiental, luz ambiental, ubicación, movimiento o comunicaciones compartidas.
2204
Recibir uno o más permisos y políticas para los dispositivos secundarios junto con el valor de autentificación principal.
2206
Determinar si se requiere autentificación secundaria en función de si se requiere una autentificación secundaria en función de una acción iniciada por el usuario, como una o más de una transacción financiera, acceso a contenido seguro y acceso a sistemas de control seguros y, de ser así, realizar la autentificación secundaria por detectar uno o más de un parámetro de reconocimiento de gestos, un parámetro de reconocimiento facial y un parámetro de reconocimiento de voz.
2208
Detectar un activador para desautentificar al usuario del dispositivo secundario y, en respuesta, desautentificar al usuario del dispositivo secundario y notificar al dispositivo principal en el que el activador para desautentificar al usuario del dispositivo secundario incluye al menos uno de: (a) un usuario inició la desautentificación del dispositivo secundario, (b) un tiempo de espera del dispositivo secundario, (c) una indicación de amenaza del dispositivo secundario representativa de un compromiso de seguridad del dispositivo secundario, (d) una pérdida de comunicación con el dispositivo principal, o (e) una violación de un permiso o política predeterminada u otra política de agrupación.
2210
Realizar transacciones financieras por cantidades autorizadas inferiores a las del dispositivo principal de la red ad hoc.

FIG. 22