(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 744 335**

(51) Int. CI.:

H04W 80/02 (2009.01)
H04L 29/08 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **19.10.2015 PCT/US2015/056179**

(87) Fecha y número de publicación internacional: **28.07.2016 WO16118199**

(96) Fecha de presentación y número de la solicitud europea: **19.10.2015 E 15791093 (6)**

(97) Fecha y número de publicación de la concesión europea: **19.06.2019 EP 3248437**

(54) Título: **Sistemas, métodos y dispositivos para la comunicación directa entre dispositivos mediante encapsulación**

(30) Prioridad:

19.01.2015 US 201562105000 P
31.03.2015 US 201562140926 P
26.06.2015 US 201514751436

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
24.02.2020

(73) Titular/es:

INTEL IP CORPORATION (100.0%)
2200 Mission College Boulevard
Santa Clara, CA 95054, US

(72) Inventor/es:

STOJANOVSKI, ALEXANDRE;
VENKATACHALAM, MUTHAIAH;
PINHEIRO, ANA LUCIA A. y
ADRANGI, FARID

(74) Agente/Representante:

LEHMANN NOVO, María Isabel

DESCRIPCIÓN

Sistemas, métodos y dispositivos para la comunicación directa entre dispositivos mediante encapsulación

Campo técnico

La presente descripción se refiere a la comunicación inalámbrica y más específicamente a la comunicación directa entre dispositivos que utilizan encapsulación. 3GPP Tdoc. R2 -145305 (Solicitud De cambio CR 131, revisión 2), "Introducción a la comunicación directa de ProSe", 3GPP TSG-RAN WG2 reunión # 88, noviembre de 2014, sugiere cambios en el PDCP para permitir la comunicación directa de ProSe a través de un enlace lateral. El documento "Estándar de uso IEEE para acceso inalámbrico en ambientes vehiculares (WAVE) - Operación multicanal", Estándar IEEE 1609.4, publicado por IEEE =, el 29-11-2006 describe una extensión del modo IEEE 802.11 WAVE que describe cómo soportar un sistema multicanal con el control de acceso de medios (MAC) y capas físicas (PHY) IEEE 802.11 a través de un canal de control (CCH) y de múltiples canales de servicio (SCH).

Compendio

La invención se define por la materia objeto de las reivindicaciones independientes. Las realizaciones ventajosas están sujetas a las reivindicaciones dependientes.

Breve descripción de los dibujos

La Fig. 1 es un diagrama esquemático que ilustra un sistema de comunicación directa conforme a las realizaciones descritas en la presente memoria.

La Fig. 2 es un diagrama esquemático que ilustra una unidad de datos del protocolo de convergencia de datos por paquetes (PDCP) conforme a las realizaciones descritas en la presente memoria.

La Fig. 3 es un diagrama de bloques de una pila de protocolos de acceso inalámbrico en entornos vehiculares (WAVE) conforme a las realizaciones descritas en la presente memoria.

La Fig. 4 es un diagrama de un control de enlace lógico/encabezado del protocolo (LLC/SNAP) de acceso a la subred para WAVE conforme a las realizaciones descritas en la presente memoria.

La Fig.5 es un diagrama de una interfaz PC5 y una pila de protocolos conforme a las realizaciones descritas en la presente memoria.

La Fig. 6 es un diagrama de proceso que ilustra la comunicación de PC5 utilizando un protocolo IP conforme a las realizaciones descritas en la presente memoria.

La Fig. 7 es un diagrama de proceso que ilustra la comunicación de PC5 con negociación de seguridad conforme a las realizaciones descritas en la presente memoria.

La Fig. 8 es un diagrama de proceso que ilustra la comunicación de PC5 sin negociación de seguridad utilizando un servidor de gestión de claves común conforme a las realizaciones descritas en la presente memoria.

La Fig. 9 es un diagrama de proceso que ilustra la comunicación de PC5 sin negociación de seguridad utilizando diferentes servidores de gestión de claves conforme a las realizaciones descritas en la presente memoria.

La Fig. 10 es un diagrama de proceso que ilustra un esquema de firmas sin certificado basado en curvas elípticas para la encriptación basado en identidad (ECCSI) conforme a las realizaciones descritas en la presente memoria.

La Fig. 11 es un diagrama de proceso que ilustra la encriptación de claves secreta de Skai-Kasahara (SAKKE) conforme a las realizaciones descritas en la presente memoria.

La Fig. 12 es un diagrama de proceso que ilustra el sistema de circuitos de dispositivos electrónicos conforme a las realizaciones descritas en la presente memoria.

La Fig. 13 es un diagrama de flujo que ilustra un método de comunicación con negociación de seguridad conforme a las realizaciones descritas en la presente memoria.

La Fig. 14 es un diagrama de flujo que ilustra un método para recibir datos con negociación de seguridad conforme a las realizaciones descritas en la presente memoria.

La Fig. 15 es un diagrama de flujo que ilustra un método de comunicación sin negociación de seguridad conforme a las realizaciones descritas en la presente memoria.

La Fig. 16 es un diagrama de flujo que ilustra un método para recibir comunicación sin negociación de seguridad conforme a las realizaciones descritas en la presente memoria.

La Fig. 17 es un diagrama esquemático de un sistema informático conforme a las realizaciones descritas en la presente memoria.

La Fig. 18 es una ilustración de ejemplo de un dispositivo móvil conforme a las realizaciones descritas en la presente memoria.

La Fig. 19 es un diagrama esquemático de un sistema informático alternativo conforme a las realizaciones descritas en la presente memoria.

Descripción detallada

A continuación se proporciona una descripción detallada de los sistemas y métodos conforme a las realizaciones de la presente descripción. Aunque se describen varias realizaciones, se debe entender que la descripción no se limita a ninguna realización.

Se describen técnicas, aparatos y métodos que permiten la comunicación de dispositivo a dispositivo (D2D) utilizando una encapsulación basada en el protocolo de convergencia de datos en paquetes (PDCP) sin direccionamiento del protocolo de Internet (IP). La comunicación no encapsulada en IP D2D PDCP puede incluir además dos formas de transferencia segura de datos. Una primera comunicación no encapsulada en IP D2D PDCP puede ser una comunicación negociada no encapsulada en IP D2D PDCP. Una segunda comunicación no encapsulada en IP D2D PDCP puede ser una comunicación no negociada no-IP D2D. La comunicación no negociada no encapsulada en IP-D2D-PDCP puede incluir una versión de un servidor de gestión de claves común (KMS) y una versión de KMS distribuida. La comunicación encapsulada se puede utilizar con diversos protocolos, incluyendo el PC5 y el acceso inalámbrico en los protocolos de los entornos vehiculares (WAVE).

Por ejemplo, un encabezado PDCP incluye un tipo de unidad de datos de servicio (tipo SDU). El tipo SDU puede definir un nuevo tipo SDU para incluir un protocolo PC5 (como el protocolo de señalización PC5). El encabezado PDCP puede utilizar el nuevo tipo de protocolo PC5 para indicar que se utilizará un protocolo PC5 que no requiere soporte de dirección IP. En su lugar, puede utilizarse una ID de capa 2 (p.ej., un identificador de capa-MAC PC5). Un transmisor UE puede enviar un mensaje de solicitud de comunicación directa a un receptor UE. El receptor UE puede realizar un procedimiento de autenticación para permitir un enlace seguro de capa 2 sobre PC5. El transmisor UE puede enviar entonces datos de usuario dentro de un mensaje de protocolo PC5 (p.ej., un mensaje de datos de usuario) como una carga útil.

En otro ejemplo, se puede modificar un tipo SDU para incluir un tipo de control de enlace lógico/protocolo (LLC/SNAP) de acceso a subred. La encapsulación de LLC/SNAP puede utilizarse entonces para identificar en el campo del tipo ethernet que se utilizará un protocolo PC5 (como el protocolo de señalización PC5). Un transmisor UE y un receptor UE están configurados para el uso de criptografía basada en identidad y dependen de una raíz común de confianza. El transmisor UE conoce la información de identificación de capa 2 ID y la información de identidad pública de un receptor UE. El transmisor UE construye un mensaje de datagrama de PC5 utilizando la información de identidad pública, firmas sin certificado basadas en curvas elípticas para la encriptación basada en identidad (ECCSI), carga útil de encriptación de clave Saai-Kasahara (SAKKE) y datos de usuario encriptados con una clave en la carga útil SAKKE. El transmisor UE envía el mensaje de datagrama de PC5 encapsulado por LLC/SNAP a través de PDCP al receptor UE.

La tecnología de comunicación móvil inalámbrica utiliza diversos estándares y protocolos para transmitir datos entre una estación base y un dispositivo móvil inalámbrico. Los estándares y protocolos del sistema de comunicación inalámbrica pueden incluir la evolución del Proyecto de asociación de 3a generación (3GPP) a largo plazo (LTE); el estándar 802.16 del Instituto de Ingeniería Eléctrica y Electrónica (IEEE), comúnmente conocido por los grupos industriales como interoperabilidad mundial para el acceso a microondas (WiMAX); y el estándar 802.11 del IEEE, comúnmente conocido por los grupos industriales como Wi-Fi. En redes de acceso radioeléctrico 3GPP (RAN) en los sistemas LTE, la estación base puede incluir Nodo B de la Red Universal de Acceso Radioeléctrico Terrestre Evolucionado (E-UTRAN) (también denominado comúnmente Nodo B evolucionado, Nodo B mejorado, eNode B, o eNB) y/o Controladores de Red Radioeléctrica (RNC) en un E-UTRAN, que se comunican con un dispositivo de comunicación inalámbrica, conocido como equipo de usuario (UE).

La transmisión de datos entre dos dispositivos (dos UE) puede realizarse utilizando el transporte IP. La versión 12 de las especificaciones 3GPP de dispositivo a dispositivo (D2D) (también conocidas como Servicios de Proximidad - (ProSe)) soporta la comunicación basada en IP [3GPP TR 23.303, 36.300]. Sin embargo, en algunos casos, el uso de IP no es un enfoque óptimo. Por ejemplo, se utiliza un pequeño dispositivo para la comunicación de equipo a equipo. Es posible que el dispositivo pequeño no sea compatible con IP, ya que se ha determinado que es demasiado costoso en términos de implementación. En otro ejemplo, los datos que deben transmitirse son tan pequeños que la sobrecarga del encabezado IP no puede justificarse.

La transmisión de datos de paquetes no-IP puede producirse entre dos dispositivos, como a través de una transmisión en el plano de usuario (p.ej., los paquetes se transmiten en el plano de usuario como PDCP-SDU). Además, los datos pueden transmitirse entre dos dispositivos mediante el transporte combinado de un paquete a un mensaje de señalización a través de un protocolo PC5 (como el protocolo de señalización PC5). Este enfoque 1) no

requiere una sobrecarga de encabezado IP necesaria por la solución actual, 2) no requiere la adición de un nuevo tipo SDU en PDCP, y 3) reutiliza el protocolo de señalización PC5 3GPP TR 23.713.

En la Fig. 1, Las comunicaciones no encapsuladas en IP D2D PDCP se muestran en un entorno 100 entre múltiples tipos de dispositivos. Las comunicaciones no encapsuladas en IP-D2D-PDCP se pueden clasificar en función de lo que se está comunicando. Mientras que D2D describe el sistema genérico (p.ej., entre un dispositivo 102 móvil y un dispositivo 104 móvil), en la definición de D2D se incluyen otras realizaciones específicas. Por ejemplo, se producen comunicaciones de dispositivo a infraestructura (D2I) entre el dispositivo 102 móvil y un sistema estacionario, como una señalización 108 vial mejorada que incluye una Unidad de carretera (RSU). En otro ejemplo, se producen comunicaciones de dispositivo a vehículo (D2V) entre el dispositivo 102 móvil y un vehículo 106. En un ejemplo, se producen las comunicaciones de vehículo a infraestructura (V2I) entre el vehículo 106 y un sistema estacionario, como la señalización 108 vial mejorada que incluye una RSU. En un ejemplo, las comunicaciones no encapsuladas en IP-PDCP son entre sensores domésticos como un teléfono móvil que controla un refrigerador. En un ejemplo, los electrodomésticos (p.ej., lavadora, secadora, aire acondicionado) están controlados por una caja de alimentación basada en el uso actual de potencia en la red de eléctrica utilizando comunicaciones no encapsuladas en IP-D2D PDCP. Otros ejemplos de intercomunicación son posibles y se contemplan, algunos de los cuales se describen adicionalmente más adelante.

Las comunicaciones no encapsuladas en IP-D2D-PDCP pueden reutilizar el protocolo de señalización PC5 [TR 23.713] u otro protocolo PC5 para permitir la comunicación entre dispositivos. Mediante la reutilización de la complejidad del dispositivo de señalización PC5 se puede reducir a medida que el dispositivo no necesita admitir IP. Las comunicaciones no encapsuladas en IP-D2D PDCP no requieren una sobrecarga de encabezado IP. Las comunicaciones no encapsuladas en IP-D2D PDCP pueden eliminar la sobrecarga de la asignación de direcciones IP durante el establecimiento del enlace. Las comunicaciones no encapsuladas en IP-D2D PDCP no requieren la adición de un nuevo tipo SDU en PDCP, pero pueden usar uno.

En la Fig. 2 se ilustra una realización 200 de la unidad de datos del protocolo PDCP en Rel-12 ProSe [3GPP R2-145305]. La unidad de datos de protocolo PDCP puede incluir un tipo SDU, una clave 204 de grupo ProSe (PGK), una identidad 206, 208 de clave de tráfico ProSe (PTK) y un número 210, 212 de secuencia PDCP (PDCP-SN). Un tipo 202 de SDU es el tipo de unidad de datos de protocolo capa-3. La entidad PDCP procesa la SDU de manera diferente dependiendo del tipo 202 de SDU. Por ejemplo, la compresión de encabezado es aplicable a la SDU IP pero no a la SDU de protocolo de resolución de dirección (ARP). La siguiente tabla muestra los tipos de SDU compatibles, que son IP y ARP. Se reservan otros valores. [R2-145305]

Tabla 1 - Tipo PDCP SDU

Bit	Descripción
000	IP
001	ARP
010-111	Reservado

Existen casos de uso en los que el uso de comunicaciones basadas en IP puede no ser práctico. Por ejemplo, en el caso de la comunicación de vehículo a vehículo (V2V) o de vehículo a infraestructura (V2I) el intercambio de datos (p.ej., varias alertas de seguridad) se limita a menudo entre un par de unidades a bordo (OBU) montadas en un vehículo, o entre una OBU y una RSU. Estas unidades son fabricadas por vendedores especializados (p.ej., fabricantes de automóviles o fabricantes de equipos de carretera), y no hay necesidad aparente de abrir el sistema a una comunidad más amplia de desarrolladores de aplicaciones. Para tales casos, el uso de IP puede añadir sobrecarga innecesaria (tal como 128 bits en el caso IPv6).

El conjunto de estándares IEEE 1609 para el acceso inalámbrico en entornos vehiculares (WAVE) permite la no-IP además de la comunicación basada en IP, como se ilustra en la pila 300 de protocolos que se muestra en la Fig. 3. Una capa 302 superior puede incluir aplicaciones 304 y 306 propietarias, aplicaciones 308 de seguridad y un sistema 310 de cobro (entre otras). Las aplicaciones pueden utilizar TCP 320 o UDP 324 a través de IPv6 322 o un protocolo de protocolo 312 de mensajes cortos WAVE (WSMP). Los protocolos 312 pueden ser encapsulados por una capa 314 LLC y soportados por una capa 326 y 316 de control de acceso de medios (MAC) y una capa 328 y 318 física.

La comunicación no basada en IP se realiza con un protocolo de mensajes dedicado denominado protocolo de mensaje corto WAVE (WSMP) como se muestra en la Fig. 4. Un encabezado 400 LLC incluye un campo 402 de acceso de servicio de destino (DSAP), un campo 404 de punto de acceso de servicio fuente (SSAP) y un campo 406 de control. Un encabezado SNAP incluye un campo 408 de identificación de protocolo y un campo 410 de tipo

ethernet. La encapsulación de LLC/SNAP utilizada en la subcapa LLC indica si la unidad de datos de protocolo superior es un paquete IP o un mensaje WSMP: el campo 410 de tipo ethernet se ajusta a 0x88DD para IPv6 o 0x88DC para WSMP. En algunas realizaciones, el WSMP puede utilizarse en una pila de protocolo D2D, que puede utilizar encapsulación LLC/SNAP.

El WSMP puede ser soportado utilizando una comunicación LTE D2D añadiendo una entrada al tipo PDCP SDU. En una primera realización, un WSMP dedicado, PC5 u otro valor de protocolo se puede añadir en el campo tipo 202 SDU como se indica en la Tabla 2. Dado el tamaño limitado del campo tipo 202 SDU, un valor dedicado para un protocolo de comunicación no-IP específico puede no ser deseable. En una segunda realización, la encapsulación LLC/SNAP de soporte en la SDU tipo 202 se puede añadir al campo tipo 202 SDU como se indica en la Tabla 3. En una tercera realización, puede ser un encabezado de encapsulación que inicia en el octeto seis una nueva encabezado de encapsulación (distinto de LLC/SNAP).

Tabla 2 - Valor WSMP dedicado en el tipo SDU

Bit	Descripción
000	IP
001	ARP
010	WSMP
011	PC5
100-111	Reservado

Tabla 3 - Soporte de encapsulación LLC/SNAP en el tipo SDU

Bit	Descripción
000	IP
001	ARP
010	LLC/SNAP
011-111	Reservado

Tabla 4 - Soporte genérico de encapsulación

Bit	Descripción
000	IP
001	ARP
010	Unidad de datos encapsulada
011-111	Reservado

El uso de WSMP, PC5 u otro protocolo puede encapsularse en un encabezamiento LLC/SNAP. Cuando el tipo 202 SDU se fija en LLC/SNAP, la unidad de datos (comenzando en el octeto seis de la Fig. 1) está encapsulada en LLC/SNAP. El uso de WSMP (PC5 u otro protocolo) se indica entonces como parte del encabezado de encapsulación LLC/SNAP (véase la Fig. 3) La ventaja de esta propuesta es que se puede utilizar para soportar otros protocolos no basados en IP. Sin embargo, en esta realización, la encapsulación de LLC/SNAP desperdicia seis de ocho octetos (p.ej., con referencia a la Fig. 3, solo se utiliza eficazmente el tipo de ethernet dos octetos para discriminar las unidades de datos de la capa superior).

La Fig. 5 muestra una realización 500 con dos dispositivos 502 y 504 que se comunican directamente entre sí, sin paquetes que tengan que viajar a través de la red central 3GPP. En la figura se muestra una pila de protocolo PC5 utilizables con D2D. La pila de protocolos puede incluir una capa 506a y 506b de protocolo de señalización PC5, una capa 508a y 508b de PDCP, un control de enlace de radioeléctrico (RLC), una capa 510a y 510b, una capa 512a y 512b de acceso medio (MAC) y una capa 514a y 514b física (PHY). No se necesita una dirección IP, ya que los dispositivos pueden ser identificados mediante la ID de capa 2 de ProSe (p.ej., un PC5 identificador 512a y 512b de capa MAC). El uso de las direcciones IP es redundante en este caso.

Por ejemplo, en 3GPP TR 23.713, la comunicación directa ProSe una a una puede realizarse estableciendo un enlace seguro de capa 2 sobre PC5 entre dos UE. Un UE tiene una ID de capa 2 para la comunicación unidifusión que se incluye en el campo ID de la capa 2 de origen de un marco que envía en el enlace de capa 2 y en una ID de capa 2 de destino de un marco que recibe en el enlace de capa 2.

Un ID de capa 2 para la comunicación de unidifusión puede ser único a nivel global o el UE puede garantizar que la ID de capa 2 sea al menos única a nivel local. Si se produce un conflicto, el UE puede detectar si la ID de capa 2 entra en conflicto con los UE adyacentes y autoasignar un nuevo ID de UE ProSe cuando se detecta un conflicto.

Un enlace de la capa 2 para la comunicación directa ProSe una a una puede ser identificado por la combinación de los ID de la capa 2 de dos UE. Un UE puede establecer múltiples enlaces de capa 2 para la comunicación directa ProSe una a una utilizando el mismo ID de capa 2.

Se propone un protocolo de señalización PC5 en 3GPP TR 23.713. Un protocolo de señalización PC5 establece un enlace seguro de capa 2 sobre PC5. Se puede añadir un tipo SDU = Protocolo de señalización PC5 a un campo de tipo SDU en PDCP.

Los mensajes del protocolo de señalización PC5 pueden enviarse en un ID de capa 2 de destino unicast, groupcast o broadcast. En la Fig. 6 se muestra un procedimiento 600 para la comunicación basada en IP. Un UE de iniciación (UE-1) 602 aprende la ID de la capa 2 de un UE par (UE-2) 604 (p.ej., escuchando los anuncios emitidos por el otro UE o realizando un procedimiento de descubrimiento ProSe) y envía un mensaje 606 de solicitud de comunicación directa al UE-2 604 para activar la autenticación mutua. El UE-2 604 inicia un procedimiento de autenticación 608 mutua. La finalización satisfactoria del procedimiento de autenticación 608 mutua completa el establecimiento del enlace seguro de capa 2 a través de PC5. Uno de los dos UE actúa como servidor DHCP o enrutador IPv6 por defecto o los UE autoasignan 610 una dirección IP local de enlace. Los datos se transmiten 612 utilizando direcciones IP sobre el plano de usuario utilizando el tipo SDU = IP.

A diferencia de la Fig. 6, las Fig. 7 -9 muestran los procedimientos para la comunicación no basada en IP. En ambos procedimientos, los datos de usuario se transportan dentro de un mensaje de protocolo de señalización PC5. Puede utilizarse un procedimiento negociado o procedimiento no negociado. En un procedimiento negociado, dos UE establecen primero un enlace seguro de capa 2. El material clave intercambiado durante el establecimiento de enlace de capa 2 se utiliza para proteger la confidencialidad y/o la integridad de los datos de usuario subsiguientes. En un procedimiento no negociado, dos UE intercambian datos sin establecer previamente un enlace de la capa 2. Un emisor afirma una identidad y la firma digitalmente en cada mensaje (p.ej., con una firma ECCSI). Opcionalmente, algunas partes del mensaje también pueden ser encriptadas y la clave de un solo disparo utilizada para la encriptación se transmite dentro del propio mensaje (p.ej., como carga útil SAKKE).

La Fig. 7 muestra un procedimiento 700 negociado. Un UE de iniciación (UE-1) 702 aprende la ID de capa 2 de un UE (UE-2) 704 (p.ej., escuchando un anuncio emitido por el otro UE o realizando un procedimiento de descubrimiento ProSe) y envía un mensaje 706 de solicitud de comunicación directa al UE-2 704 para activar la autenticación mutua. El UE-2 704 inicia el procedimiento de autenticación mutua. La finalización satisfactoria del procedimiento de autenticación completa el establecimiento de un enlace 708 seguro de capa 2 a través de PC5. Los datos se transmiten al enviar datos de usuario dentro de un mensaje 710 de protocolo de señalización PC5 (p.ej., utilizando un mensaje de datos de usuario PC5). En algunas realizaciones, un tipo SDU puede establecerse en un protocolo de señalización PC5. Los datos de usuario pueden ser transportados como parte de la carga útil del mensaje 710 de protocolo de señalización PC5 al que se hace referencia como datos de usuario PC5.

En la Fig. 8, se muestra un ejemplo de un procedimiento 800 no negociado. Los UE 802 y 804 están configurados para el uso de criptografía basada en identidad y dependen de una raíz común de confianza 806, a la que se hace referencia como Sistema de gestión de claves. Los UE 802 y 804 están configurados para el uso de un esquema de firma ECCSI (IETF RFC 6507 y descrito en relación con la Fig. 10) y el algoritmo SAKKE (IETF RFC 6508 y descrito en relación con la Fig. 11) como mecanismos para la firma digital de una identidad declarada y un intercambio seguro de una clave secreta. Además de una identidad de usuario pública (a la que se hace referencia aquí como Información de Usuario-1 o Información de Usuario-2, ambas codificadas en un formato user@realm con una marca de tiempo anexo o cualquier otro formato que sea compatible con las directrices de IETF RFC 6509), los UE 802 y 804 están configurados con la siguiente información:

KPAK - Clave de autenticación pública KMS (IETF RFC 6507)

SSK- Clave de firma secreta (IETF RFC 6507)

PVT - Token de validación pública (IETF RFC 6507)

Clave Pública KMS (IETF RFC 6508)

RSK - Clave secreta del receptor (IETF RFC 6508)

Un UE de iniciación (UE-1) 802 aprende un ID de capa 2 de un UE par (UE-2) 804 y la identidad pública del usuario UE-2 804 (Información de Usuario-2). Por ejemplo, el UE-1 802 puede escuchar anuncios emitidos por el UE-2 804 o realizando un procedimiento de descubrimiento ProSe.

El UE-1 802 envía un datagrama 808 PC5 que incluye parámetros como Información de Usuario-1 SIGN, SAKKE, o mensaje de datos de usuario al UE-2 804. El parámetro de Información de Usuario-1 es una identidad pública que es confirmada por el usuario del UE-1 802. El parámetro SIGN es una firma ECCSI del mensaje del datagrama 808 PC5. La firma puede calcularse sobre todos o un subconjunto de los parámetros del mensaje. En una realización, la firma se calcula sobre el parámetro de Información de Usuario-1. Un proceso para calcular la firma ECCSI se describe en IETF RFC 6507, que utiliza los parámetros KPAK, SSK y SVT.

En algunas realizaciones, es opcional una carga útil SAKKE. Se puede utilizar si el parámetro de datos de usuario que se transporta en el mismo mensaje va a ser cifrado. Por ejemplo, el UE-1 802 genera una clave de encriptación (también conocida como Valor Secreto Compartido (SSV) en IETF RFC 6508) y la codifica en una carga útil SAKKE de acuerdo con el algoritmo descrito en IETF RFC 6508, utilizando la clave pública KMS y la identidad pública del usuario del UE-2 804 (Información de Usuario-2). Un parámetro de datos de usuario designa los datos de usuario. Está encriptado con la clave de encriptación proporcionada dentro de la carga útil SAKKE.

La Fig. 9 muestra un procedimiento 900 para datos no negociados no-IP a través de PC5 con UE dependiendo de diferentes servidores de gestión de claves (KMS). En algunos despliegues, la población de UE 902 y 904 puede dividirse entre varios KMS. Esto puede ser debido a que los KMS son accionados por diferentes administraciones o a que la población de UE es tan grande que no resulta práctico manejarlos con un solo.

En estos escenarios de despliegue múltiple de KMS, un UE pertenece a un KMS específico que se identifica mediante un único identificador KMS (KMS ID). El KMS ID puede ser codificado como URI (p.ej., en formato server@realm) que es una cadena de texto. Sin embargo, si el conjunto de KMS que manejan la población global de UE depende de un único "superadministrador" puede ser posible utilizar ID de KMS mucho más cortos (p.ej., del orden de uno o dos octetos).

En la realización mostrada, un UE de iniciación (UE-1) 902 y un UE par (UE-2) 904 se configuran para el uso de criptografía basada en identidad y dependen de diferentes KMS. En una realización, se configuran para el uso del esquema de firma ECCSI (IETF RFC 6507) y el algoritmo SAKKE (IETF RFC 6508) como mecanismos para la firma digital de una identidad afirmada y un intercambio seguro de una clave secreta. Además de su identidad de usuario pública (a la que se le hace referencia aquí como Información de Usuario-1 o Información de Usuario-2, ambas codificadas en un formato user@realm con una marca de tiempo aneja, o cualquier otro formato que sea compatible con las directrices en IETF RFC 6509), cada UE en la realización está configurado con la siguiente información:

Para cada KMS a la que pertenece el UE se configura con los siguientes parámetros:

KMS ID (identificador único de la KMS; en algunas realizaciones puede deducirse de la Información de Usuario)

KPAK - Clave de autenticación pública KMS (IETF RFC 6507)

SSK- Clave de firma secreta (IETF RFC 6507)

PVT - Token de validación pública (IETF RFC 6507)

Clave Pública KMS (IETF RFC 6508)

RSK - Clave secreta del receptor (IETF RFC 6508)

Para todas las demás KMS el UE está configurado con la siguiente información:

Clave Pública KMS (IETF RFC 6508)

El UE-1 902 y el UE-2 904 dependen de una raíz común de confianza 906. El UE-1 902 aprende la ID de la capa 2 del par UE -2 904 y la identidad pública del usuario del UE-2 904 (Información de Usuario-2) y la ID de KMS-2 del KMS a la que pertenece el usuario del UE-2 904 (obsérvese que la ID de KMS-2 puede deducirse de la Información de Usuario-2 en algunas realizaciones). Esto se puede realizar, por ejemplo, escuchando los anuncios emitidos por el UE par o realizando un procedimiento de descubrimiento ProSe. El UE-1 902 envía un mensaje de datagrama PC5 908 con parámetros de KMS-1 ID, Información de Usuario-1, SIGN, SAKKE y datos de usuario al UE-2 904. El parámetro KMS-1 ID es el identificador de la KMS a la que pertenece el usuario del UE-1 902 (obsérvese que la ID de KMS-1 puede ser deducida de la Información de Usuario-1). El parámetro de Información de Usuario-1 es una

identidad pública que es confirmada por el usuario del UE-1 902. El parámetro SIGN es una firma ECCSI del mensaje de datagrama PC5 908. La firma puede calcularse sobre todos o un subconjunto de los parámetros del mensaje. En una realización, la firma se calcula sobre el parámetro de Información de Usuario-1. Un proceso para calcular la firma ECCSI se describe en IETF RFC 6507; hace uso de los parámetros KPAK SSK y SVT correspondientes a la KMS a la que pertenece el UE-1 902.

En una realización, puede ser opcional una carga útil SAKKE. Se utiliza si el parámetro de datos del usuario transportado en el mismo mensaje necesita ser encriptado. En una realización, el UE-1 902 genera una clave de encriptación (también conocida como Valor Secreto Compartido (SSV) en RFC 6508) y la codifica en una carga útil SAKKE de acuerdo con el algoritmo descrito en IETF RFC 6508 utilizando la clave pública KMS de KMS-2 (es decir, la KMS a la que pertenece el usuario del UE-2 904) y la identidad pública del usuario del UE-2 904 (Información de Usuario-2). Un parámetro de datos de usuario designa los datos de usuario. Puede encriptarse con la clave de encriptación proporcionada dentro de la carga útil SAKKE.

Los procedimientos no negociados descritos en la Fig. 8 y la Fig. 9 también pueden utilizarse en caso de que los datos de usuario sean encapsulados en un encabezado de encapsulación genérico (es decir, no tienen que ser transportados como parte de la carga útil del protocolo de señalización PC5). En este caso la presencia del encabezado de encapsulación se indica mediante un valor apropiado del campo de tipo SDU en el encabezado PDCP.

Los procedimientos no negociados descritos en la figura 8 y la figura 9 también pueden utilizarse en caso de que los datos de usuario sean un paquete IP. En este caso, de nuevo, se señala la presencia del encabezado de encapsulación por un valor apropiado del campo de tipo SDU en el encabezado PDCP. El valor tipo SDU implica también que los datos encapsulados son un paquete IP.

La Fig. 10 muestra una realización de un esquema 1000 de firma ECCSI en IETF RFC 6507 que permite que un Firmante 1004 firme un mensaje (M) 1016 y luego sea verificado por un Verificador 1006 utilizando criptografía basada en identidad. El Firmante 1004 y el Verificador 1006 tienen una raíz común de confianza conocida como servidor de gestión de claves que incluye una KMS 1002. La KMS 1002 posee una clave de autenticación pública KMS (KPAK) 1008 que es conocida por los usuarios de la KMS 1002. Además, cada usuario tiene una identidad públicamente conocida (p.ej., una ID_ s 1014 es la identidad pública del Firmante 1004 (ID_r, no mostrada, es la identidad pública del receptor).

Un usuario que desea firmar 1020 digitalmente sus mensajes puede solicitar la KMS 1002 para un par de claves de firma secreta (SSK) 1012 y un token de validación pública (PVT) 1010. El Firmante 1004 utiliza los parámetros KPAK 1008, SSK 1012 y PVT 1010 para producir una firma digital (SIGN) 1018 de acuerdo con el proceso descrito en IETF RFC 6507. En algunas realizaciones, el parámetro PVT 1010 no es secreto y se incluye dentro de la carga útil de SIGN 1018 como texto transparente. Tras la recepción de un mensaje firmado digitalmente, el Verificador 1006 utiliza la identidad pública 1004 de KPAK 1008 (la ID_s 1014) para realizar un proceso 1022 de verificación como se describe en IETF RFC 6507.

La Fig. 11 muestra la realización de un algoritmo SAKKE 1100 definido en IETF RFC 6508 que permite el intercambio encriptado de una clave secreta compartida entre un Emisor 1104 y un Receptor 1106 utilizando criptografía basada en identidad. El Emisor 1104 y el Receptor 1106 tienen de nuevo una raíz común de confianza (p.ej., una KMS 1102). La KMS 1102 posee una clave pública KMS 1108 que es conocida por los usuarios. Cada usuario tiene una identidad públicamente conocida (p.ej., una ID_r 1114 es la identidad pública del Receptor 1106; la ID_s, no mostrada, es la identidad pública del Emisor 1104). Para permitir que un usuario desencripte mensajes, el usuario proporciona a la KMS 1102 una solicitud de una clave secreta de receptor (RSK) 1110. El Emisor 1104 utiliza la clave 1108 pública KMS y la identidad pública del receptor 1106 (la ID_r 1114) para codificar un valor secreto compartido (SSV) 1110 de acuerdo con el proceso descrito en IETF RFC 6508. Se hace referencia a una carga útil encriptada resultante como una carga útil SAKKE 1116. Tras la recepción de la carga útil SAKKE 1116, el Receptor 1106 utiliza la clave pública KMS 1108, la RSK 1110 y la identidad pública del Receptor 1106 (la ID_r 1114) para realizar el algoritmo de descifrado como se describe en IETF RFC 6508.

La Fig. 12 ilustra un sistema de circuitos 1202 de dispositivos electrónicos que puede ser un sistema de circuitos eNB, un sistema de circuitos UE o algún otro tipo de sistema de circuitos que forma un sistema 1200 de acuerdo con diversas realizaciones. En realizaciones, el sistema de circuitos 1202 de dispositivos electrónicos puede ser, o puede incorporarse o de otra manera formar parte de un eNB, un UE, o algún otro tipo de dispositivo electrónico. En realizaciones, el sistema de circuitos de dispositivos electrónicos 1202 puede incluir un sistema de circuitos 1204 de transmisión de radio y un sistema de circuitos 1206 de recepción acoplado a un sistema de circuitos 1208 de control. En realizaciones, el sistema de circuitos 1204 de transmisión y/o el sistema de circuitos 1206 de recepción pueden ser elementos o módulos del sistema de circuitos del transceptor, como se muestra. El sistema de circuitos 1202 de dispositivos electrónicos puede estar acoplado con uno o más elementos 1210a a 1210x de antena de una o más antenas. El sistema de circuitos 1202 de dispositivos electrónicos y/o los componentes del sistema de circuitos 1202 de dispositivos electrónicos pueden estar configurados para realizar operaciones similares a las descritas en otra parte de la presente descripción

En realizaciones en donde el sistema de circuitos 1202 de dispositivos electrónicos es un UE o forma parte de o está incorporado de otro modo en un UE, el sistema de circuitos 1204 de transmisión puede ser capaz de transmitir, a un segundo equipo de usuario (UE) basado en una identidad de la capa 2 del segundo UE, una solicitud para el establecimiento de un enlace seguro para la comunicación a través de PC5. El sistema de circuitos 1206 de recepción puede ser capaz de recibir, desde el segundo UE, una indicación de que se ha completado el establecimiento del enlace seguro por el segundo UE. El sistema de circuitos 1208 de control puede ser capaz de encapsular un paquete de datos dentro de un mensaje de protocolo de señalización PC5.

Adicionalmente o alternativamente, el sistema de circuitos 1204 de transmisión puede ser capaz de transmitir, por el segundo UE a un primer UE basado en una identidad de la capa 2 del segundo UE, una indicación de que el segundo UE ha completado el establecimiento de un enlace seguro para la comunicación directa de datos con el primer UE a través de PC5, a petición del primer UE. El sistema de circuitos 1206 de recepción puede ser capaz de recibir, del primer UE basándose en una transmisión de la indicación de finalización, un paquete de datos dentro de un mensaje de protocolo de señalización PC5 en el enlace seguro a través de PC5.

Adicionalmente o alternativamente, el sistema de circuitos 1208 de control puede ser capaz de generar una transmisión de datos que incluya datos como datos encapsulados y un encabezado de encapsulación que incluya una identidad pública afirmada de un usuario del primer UE, una firma digital relacionada con el primer UE, una clave de encriptación utilizada para encriptar los datos si los datos están encriptados y/o un servidor de gestión de claves. El sistema de circuitos 1204 de transmisión puede ser capaz de transmitir la transmisión de datos al segundo UE.

Adicionalmente o alternativamente, el sistema de circuitos 1206 de recepción puede ser capaz de recibir una transmisión de datos que incluye datos encapsulados y un encabezado de encapsulación. El sistema de circuitos 1208 de control puede ser capaz de identificar datos en los datos encapsulados basándose en una identidad pública afirmada de un usuario del primer UE, una firma digital relacionada con el primer UE, una clave de encriptación utilizada para encriptar los datos si los datos están encriptados y/o un servidor de gestión de claves en el encabezado de encapsulación.

Como se utiliza en la presente documento, el término "sistema de circuitos" puede referirse a, forma parte de, o incluir un circuito integrado de aplicaciones específicas (ASIC), un circuito electrónico, un procesador (compartido, dedicado o de grupo) y/o memoria (compartida, dedicada o de grupo) que ejecuta uno o más programas de software o firmware, un circuito lógico de combinación, y/u otros componentes de hardware adecuados que proporcionan la funcionalidad descrita. En algunas realizaciones, el sistema de circuitos de dispositivos electrónicos puede ser implementado en, o funciones asociadas con el sistema de circuitos pueden ser implementados por, uno o más módulos de software o firmware.

Método 1

En algunas realizaciones, el sistema de circuitos 1202 de dispositivos electrónicos de la Fig. 12. puede configurarse para realizar uno o más procesos tales como el proceso 1300 de la Fig. 13. Por ejemplo, en realizaciones en donde el sistema de circuitos 1202 de dispositivos electrónicos es un UE, o está incorporado o forma parte de UE, el proceso 1300 puede incluir un método de comunicación directa de datos entre un primer equipo de usuario (UE) y un segundo UE. El proceso 1300 puede incluir la identificación 1302, por el primer UE, una identidad de capa 2 del segundo UE. El proceso 1300 puede incluir además el inicio 1304, por el primer UE, el establecimiento de un enlace seguro para la comunicación con el segundo UE a través de PC5. El proceso 1300 puede incluir además la recepción 1306, por el primer UE, una indicación de que se ha completado el establecimiento del enlace seguro por el segundo UE. El proceso 1300 puede incluir además el encapsulado 1308, por el primer UE, un paquete de datos dentro de un mensaje de protocolo de señalización PC5.

Adicionalmente o alternativamente, el sistema de circuitos 1202 de dispositivos electrónicos de la Fig. 12 puede configurarse para realizar uno o más procesos tales como el proceso 1400 de la Fig. 14. Por ejemplo, en realizaciones en donde el sistema de circuitos 1202 de dispositivos electrónicos es un UE, o está incorporado o forma parte de UE, el proceso 1400 puede incluir un método de comunicación directa de datos entre un primer equipo de usuario (UE) y un segundo UE. El proceso 1400 puede incluir la recepción 1402, por el segundo UE del primer UE basado en una identidad de la capa 2 del segundo UE, una solicitud para el establecimiento de un enlace seguro para la comunicación con el segundo UE a través de PC5. El proceso 1400 puede incluir además completar 1404, por el segundo UE basado en la solicitud, el establecimiento del enlace seguro. El proceso 1400 puede incluir además la transmisión 1406, por el segundo UE, una indicación de que se ha completado el establecimiento del enlace seguro por el segundo UE. El proceso 1400 puede incluir además la recepción 1408, por el segundo UE del primer UE basado en la finalización del establecimiento del enlace seguro, un paquete de datos dentro de un mensaje de protocolo de señalización PC5 en el enlace seguro a través de PC5.

Adicionalmente o alternativamente, el sistema de circuitos 1202 de dispositivos electrónicos de la Fig. 12 puede configurarse para realizar uno o más procesos tales como el proceso 1500 de la Fig. 15. Por ejemplo, en realizaciones en donde el sistema de circuitos 1202 de dispositivos electrónicos es un UE, o está incorporado o forma parte de un UE, el proceso 1500 puede incluir un método de comunicación directa de datos entre un primer

equipo de usuario (UE) y un segundo UE sin el establecimiento previo de un enlace seguro de la capa 2 entre el primer UE y el segundo UE y basado en el uso de la criptografía basada en la identidad. El proceso 1500 puede incluir el descubrimiento 1502 de un segundo UE. El proceso 1500 puede incluir la generación 1504, por el primer UE, de una transmisión de datos que incluye datos como datos encapsulados y un encabezado de encapsulación que incluye una identidad pública afirmada de un usuario del primer UE, una firma digital relacionada con el primer UE, una clave de encriptación utilizada para encriptar los datos si los datos están encriptados y/o un servidor de gestión de claves. El proceso 1500 puede incluir además la transmisión 1506, por el primer UE, de datos al segundo UE.

Adicionalmente o alternativamente, el sistema de circuitos 1202 de dispositivos electrónicos de la Fig. 12. Puede configurarse para realizar uno o más procesos tales como el proceso 1600 de la Fig. 16. Por ejemplo, en realizaciones en donde el sistema de circuitos 1202 de dispositivos electrónicos es un UE, o está incorporado o forma parte de un UE, el proceso 1600 puede incluir un método de comunicación directa de datos entre un primer equipo de usuario (UE) y un segundo UE sin el establecimiento previo de un enlace seguro de la capa 2 entre el primer UE y el segundo UE y basado en el uso de la criptografía basada en la identidad. El proceso 1600 puede incluir la recepción 1602, por el segundo UE, de una transmisión de datos que incluye datos encapsulados y un encabezado de encapsulación. El proceso 1600 puede incluir además la identificación 1604, por el segundo UE, de datos en los datos encapsulados basados en una identidad pública afirmada de un usuario del primer UE, una firma digital relacionada con el primer UE, una clave de encriptación utilizada para encriptar los datos si los datos están encriptados y/o un servidor de gestión de claves en el encabezado de encapsulación. El proceso 1600 puede incluir la decodificación de los datos 1606.

Las realizaciones descritas en la presente pueden implementarse en un sistema utilizando cualquier hardware y/o software adecuadamente configurado. La Fig. 17 ilustra, para una realización, un ejemplo de sistema 1700 que comprende un sistema de circuitos 1714 de radiofrecuencia (RF), un sistema de circuitos 1712 de banda base, un sistema de circuitos 1710 de aplicación, una memoria/almacenamiento 1716, una pantalla 1702, una cámara 1704, un sensor 1706 y una interfaz 1708 de entrada/salida (E/S), acoplados entre sí al menos como se muestra.

El sistema de circuitos 1710 de aplicación puede incluir circuitos tales como, entre otros, uno o más procesadores de un solo núcleo o de varios núcleos. El(los) procesador(es) puede(n) incluir cualquier combinación de procesadores de propósito general y procesadores dedicados (p.ej., procesadores gráficos, procesadores de aplicaciones, etc.) Los procesadores pueden acoplarse con la memoria/almacenamiento 1716 y configurarse para ejecutar instrucciones almacenadas en la memoria/almacenamiento 1716 para permitir varias aplicaciones y/o sistemas operativos que se ejecutan en el sistema 1700.

El sistema de circuitos 1712 de banda base puede incluir circuitos tales como, entre otros, uno o más procesadores de un solo núcleo o de varios núcleos. El(los) procesador(es) puede(n) incluir un procesador de banda base. El sistema de circuitos 1712 de banda base puede manejar varias funciones de radiocontrol que permiten la comunicación con una o más redes de radio a través del sistema de circuitos 1714 de RF. Las funciones de control de radio pueden incluir, entre otras, modulación de señal, codificación, decodificación, cambio de radiofrecuencia, etc. En algunas realizaciones, el sistema de circuitos 1712 de banda base puede proporcionar una comunicación compatible con una o más tecnologías de radio. Por ejemplo, en algunas realizaciones el sistema de circuitos 1712 de banda base puede soportar la comunicación con una Red Universal de Acceso de Radio Terrestre (E-UTRAN) y/o otra red de área metropolitana inalámbrica (WMAN), una red de área local inalámbrica (WLAN) y una red de área personal inalámbrica (WPAN). Las realizaciones en las cuales el sistema de circuitos 1712 de banda base está configurado para soportar comunicaciones de radio de más de un protocolo inalámbrico pueden denominarse como sistema de circuitos multimodo de banda base.

En diversas realizaciones, el sistema de circuitos 1712 de banda base puede incluir sistemas de circuitos para operar con señales que no se consideran estrictamente en una frecuencia de banda base. Por ejemplo, en algunas realizaciones, el sistema de circuitos 1712 de banda base puede incluir sistemas de circuitos para operar con señales que tienen una frecuencia intermedia que está entre una frecuencia de banda base y una radiofrecuencia.

El sistema de circuitos 1714 de RF puede permitir la comunicación con redes inalámbricas utilizando radiación electromagnética modulada a través de un medio no sólido. En diversas realizaciones, el sistema de circuitos 1714 de RF puede incluir conmutadores, filtros amplificadores, etc. para facilitar la comunicación con la red inalámbrica.

En diversas realizaciones, el sistema de circuitos 1714 de RF puede incluir sistemas de circuitos para operar con señales que no se consideran estrictamente en una radiofrecuencia. Por ejemplo, en algunas realizaciones, el sistema de circuitos 1714 de RF puede incluir sistemas de circuitos para operar con señales que tienen una frecuencia intermedia que está entre una frecuencia de banda base y una radiofrecuencia.

En diversas realizaciones, los sistemas de circuitos de transmisión, los sistemas de circuitos de control y/o los sistemas de circuitos de recepción analizados o descritos en la presente pueden estar incorporados en su totalidad o parcialmente en uno o más de los sistemas de circuitos 1714 de RF, en los sistemas de circuitos 1712 de banda base y/o en los sistemas de circuitos 1710 de aplicación. Como se utiliza en la presente, el término "sistema de circuitos" puede referirse a, ser parte de, o incluir un circuito integrado de aplicación específica (ASIC), un circuito

electrónico, un procesador (compartido dedicado, o grupo) y/o memoria (compartida, dedicada o de grupo) que ejecutan uno o más programas de software o firmware, un circuito lógico de combinación y/u otros componentes de hardware adecuados que proporcionan la funcionalidad descrita. En algunas realizaciones, el sistema de circuitos de dispositivos electrónicos puede ser implementado en, o funciones asociadas con el sistema de circuitos pueden ser implementados por, uno o más módulos de software o firmware.

En algunas realizaciones, algunos o todos los componentes constitutivos de los sistemas de circuitos 1712 de banda base, los sistemas de circuitos 1710 de aplicación y/o la memoria/almacenamiento 1716 pueden implementarse juntos en un sistema en un chip (SOC).

La memoria/almacenamiento 1716 puede utilizarse para cargar y almacenar datos y/o instrucciones. La memoria/almacenamiento 1716 para una realización puede incluir cualquier combinación de memoria volátil adecuada (p.ej., memoria dinámica de acceso aleatorio (DRAM)) y/o memoria no volátil (p.ej., memoria flash).

En varias realizaciones, la interfaz 1708 de E/S puede incluir una o más interfaces de usuario diseñadas para permitir la interacción del usuario con el sistema 1700 y/o las interfaces de componentes periféricos diseñadas para permitir la interacción de componentes periféricos con el sistema 1700. Las interfaces de usuario pueden incluir, entre otros, un teclado físico o teclado numérico, un panel táctil, un altavoz, un micrófono, etc. Las interfaces de componentes periféricos pueden incluir, entre otros, un puerto de memoria no volátil, un puerto bus serie universal (USB), un conector de audio y una interfaz de suministro de energía.

En varias realizaciones el sensor 1706 puede incluir uno o más dispositivos sensores para determinar las condiciones ambientales y/o la información de localización relacionada con el sistema 1700. En algunas realizaciones, los sensores 1706 pueden incluir, entre otros, un sensor giroscópico, un acelerómetro, un sensor de proximidad, un sensor de luz ambiental y una unidad de posicionamiento. La unidad de posicionamiento también puede ser parte de, o interactuar con, el sistema de circuitos 1712 de banda base y/o el sistema de circuitos 1714 de RF para comunicarse con componentes de una red de posicionamiento, p.ej., un satélite del sistema de posicionamiento global (GPS).

En diversas realizaciones, la pantalla 1702 puede incluir una pantalla (p.ej., una pantalla de cristal líquido, una pantalla táctil, etc.).

En diversas realizaciones, el sistema 1700 puede ser un dispositivo informático móvil tal como, entre otros, un dispositivo informático portátil, un dispositivo informático comprimido, un netbook, un ultrabook, un teléfono inteligente, etc. En diversas realizaciones el sistema 1700 puede tener más o menos componentes y/o diferentes arquitecturas.

En diversas realizaciones, el sistema 1700 puede ser un dispositivo informático móvil, tal como, entre otros, un dispositivo informático portátil, un dispositivo informático comprimido, un netbook, un ultrabook, un teléfono inteligente, etc. En diversas realizaciones el sistema 1700 puede tener más o menos componentes y/o diferentes arquitecturas. Por ejemplo, en algunas realizaciones el sistema de circuitos 1714 de RF y/o el sistema de circuitos 1712 de banda base pueden estar incorporados en sistemas de circuitos de comunicación (no mostrados). Los sistemas de circuitos de comunicación pueden incluir circuitos tales como, entre otros, procesadores de uno o varios núcleos de un núcleo o de núcleos y circuitos lógicos para proporcionar técnicas de procesamiento de señales, por ejemplo, codificación, modulación, filtración, conversión, amplificación, etc. adecuadas para la interfaz de comunicación apropiada sobre la que llevará a cabo las comunicaciones. Los sistemas de circuitos de comunicación pueden comunicarse a través de medios de comunicación alámbricos, ópticos o inalámbricos. En realizaciones en las que el sistema 1700 está configurado para la comunicación inalámbrica, el sistema de circuitos de comunicación puede incluir el sistema de circuitos 1714 de RF y/o el sistema de circuitos 1712 de banda base para proporcionar comunicación compatible con una o más tecnologías de radio. Por ejemplo, en algunas realizaciones, el sistema de circuitos de comunicación puede soportar la comunicación con un E-UTRAN y/u otras WMAN, una WLAN, y una WPAN.

Las realizaciones de tecnología descritas en la presente pueden describirse como como relacionadas con los estándares de evolución a largo plazo (LTE) o LTE avanzado (LTE-A) del proyecto de asociación de tercera generación (3GPP). Por ejemplo, pueden utilizarse los términos o entidades tales como eNodeB (eNB), entidad de gestión de movilidad (MME), equipo de usuario (UE), etc., que pueden considerarse términos o entidades relacionados con LTE. Sin embargo, en otras realizaciones la tecnología puede utilizarse en o estar relacionada con otras tecnologías inalámbricas tales como la tecnología inalámbrica 802.16 (WiMax) del Instituto de Ingeniería Eléctrica y Electrónica (IEEE), la tecnología inalámbrica IEEE 802.11 (Wi-Fi), diversas tecnologías inalámbricas, tales como el sistema mundial de comunicaciones móviles (GSM), las velocidades de datos mejoradas para la evolución del GSM (EDGE), la red de acceso radioeléctrico GSM EDGE (GERAN), el sistema universal de telecomunicaciones móviles (UMTS), la red de acceso radioeléctrico terrestre UMTS (UTRAN), u otras tecnologías 2G, 3G, 4G, 5G, etc., que ya están desarrolladas o están por desarrollar. En esas realizaciones, en donde se utilizan términos relacionados con LTE tales como eNB, MME, UE, etc. pueden utilizarse una o más entidades o componentes que pueden considerarse equivalentes o aproximadamente equivalentes a uno o más de los términos o entidades basados en LTE.

La Fig. 18 es una ilustración de ejemplo de un dispositivo 1800 móvil, tal como un UE, una estación móvil (MS), un dispositivo móvil inalámbrico, un dispositivo móvil de comunicación, una tableta, un teléfono u otro tipo de dispositivo móvil inalámbrico. El dispositivo 1800 móvil puede incluir una o más antenas configuradas para comunicarse con una estación de transmisión, tal como una estación base (BS), un eNB, una unidad de banda base (BBU), un encabezado de radio remoto (RRH), un equipo de radio remoto (RRE), una estación de retransmisión (RS), un equipo de radio (RE), u otro tipo de punto de acceso de red de área extensa inalámbrica (WWAN). El dispositivo 1800 móvil puede configurarse para comunicarse utilizando al menos un estándar de comunicación inalámbrica que incluye 3GPP LTE, WiMAX, HSPA, Bluetooth, y Wi-Fi. El dispositivo 1800 móvil puede comunicarse utilizando antenas separadas para cada estándar de comunicación inalámbrica o antenas compartidas para múltiples estándares de comunicación inalámbrica. El dispositivo 1800 móvil puede comunicarse en una WLAN, una WPAN y/o una WWAN.

La Fig. 18 también proporciona una ilustración de un micrófono y uno o más altavoces que pueden ser utilizados para la entrada y salida de audio del dispositivo 1800 móvil. La pantalla de visualización puede ser una pantalla de cristal líquido (LCD) u otro tipo de pantalla, tal como una pantalla de diodo orgánico de emisión de luz (OLED). La pantalla de visualización puede estar configurada como pantalla táctil. La pantalla táctil puede utilizar una tecnología capacitiva, resistiva u otro tipo de tecnología de pantalla táctil. Un procesador de aplicaciones y un procesador de gráficos pueden acoplarse a la memoria interna para proporcionar capacidades de procesamiento y presentación. También se puede utilizar un puerto de memoria no volátil para proporcionar opciones de entrada/salida de datos a un usuario. El puerto de memoria no volátil también puede utilizarse para ampliar las capacidades de memoria del dispositivo 1800 móvil. Puede integrarse un teclado con el dispositivo 1800 móvil o conectarse de manera inalámbrica al dispositivo 1800 móvil para proporcionar una entrada de usuario adicional. También se puede proporcionar un teclado virtual utilizando la pantalla táctil.

La Fig. 19 es un diagrama esquemático de un sistema 1900 informático. El sistema 1900 informático puede ser visto como un bus de paso de información que conecta diversos componentes. En la realización mostrada, el sistema 1900 informático incluye un procesador 1902 que tiene lógica para procesar instrucciones. Las instrucciones pueden ser almacenadas en y/o recuperadas de una memoria 1906 y un dispositivo de almacenamiento 1908 que incluye un medio de almacenamiento legible por ordenador. Las instrucciones y/o datos pueden llegar desde una interfaz 1910 de red que puede incluir capacidades alámbricas 1914 o inalámbricas 1912. Las instrucciones y/o datos también pueden provenir de una interfaz 1916 E/S que puede incluir cosas tales como tarjetas de expansión, buses secundarios (p.ej., USB), dispositivos, etc. Un usuario puede interactuar con el sistema 1900 informático a través de los dispositivos de interfaz 1918 de usuario y un sistema 1904 de renderizado que permite al ordenador recibir y proporcionar retroalimentación al usuario.

Se debe reconocer que el protocolo de señalización PC5 se ha utilizado como ejemplo de un protocolo PC5 que puede utilizarse. También se pueden utilizar otros protocolos PC5, identificados en campos, etc.

Las realizaciones e implementaciones de los sistemas y métodos descritos en la presente pueden incluir varias operaciones, las cuales pueden estar incorporadas en instrucciones ejecutables por máquina que serán ejecutadas por un sistema informático. Un sistema informático puede incluir una o más ordenadores de propósito general o de propósito especial (u otros dispositivos electrónicos). El sistema informático puede incluir componentes de hardware que incluyen lógica específica para realizar las operaciones o pueden incluir una combinación de hardware software y/o firmware.

Los sistemas informáticos y los ordenadores de un sistema informático pueden conectarse a través de una red. Las redes adecuadas para la configuración y/o el uso como se describe en la presente incluyen una o más redes de área local, redes de área extendida, redes de área metropolitana y/o redes de Internet o IP, tales como la red mundial, un Internet privado, un Internet seguro, una red de valor añadido, una red virtual privada, una extranet, una intranet o incluso máquinas autónomas que se comunican con otras máquinas mediante el transporte físico de medios. En particular, se puede formar una red adecuada a partir de partes o totalidades de dos o más redes diferentes, incluidas las redes que utilizan hardware y tecnologías de comunicación de red dispares.

Una red adecuada incluye un servidor y uno o más clientes; otras redes adecuadas pueden contener otras combinaciones de servidores, clientes y/o nodos de pares, y un determinado sistema informático puede funcionar como cliente y como servidor. Cada red incluye al menos dos ordenadores o sistemas informáticos, tales como el servidor y/o los clientes. Un sistema informático puede incluir una estación de trabajo, un ordenador portátil, un ordenador móvil desconectable, un servidor, un ordenador central, un clúster, el denominado "ordenador de red" o "cliente ligero", una tableta, un teléfono inteligente, un asistente digital personal u otro dispositivo informático portátil, un dispositivo o aparato electrónico de consumo "inteligente", un dispositivo médico o una combinación de los mismos.

Las redes adecuadas pueden incluir software de comunicaciones o de redes, tal como el software disponible de Novell®, Microsoft® y otros vendedores, y pueden funcionar utilizando TCP/IP, SPX, IPX, y otros protocolos sobre cables de par trenzado, coaxiales o de fibra óptica, líneas telefónicas, ondas de radio, satélites, relés de microondas, líneas eléctricas de CA moduladas, transferencia de medios físicos, y/u otros "cables" de transmisión de datos

conocidos por los expertos en la técnica. La red puede abarcar redes más pequeñas y/o ser conectable a otras redes a través de una pasarela o mecanismo similar.

Diversas técnicas, o ciertos aspectos o porciones de las mismas, pueden tomar la forma de código de programa (es decir, instrucciones) materializados en medios tangibles, tales como disquetes, CD-ROM, discos duros, tarjetas magnéticas u ópticas, dispositivos de memoria de estado sólido, un medio de almacenamiento legible por ordenador no transitorio, o cualquier otro medio de almacenamiento legible por máquina en donde, cuando el código de programa es cargado y ejecutado por una máquina, tal como un ordenador, la máquina se convierte en un aparato para la práctica de las diversas técnicas. En el caso de la ejecución del código de programa en ordenadores programables, el dispositivo informático puede incluir un procesador, un medio de almacenamiento legible por el procesador (incluidos los elementos de memoria y/o almacenamiento volátiles y no volátiles), al menos un dispositivo de entrada y al menos un dispositivo de salida. Los elementos de memoria y/o memoria volátiles y no volátiles pueden ser una RAM, una EPROM, una unidad flash, una unidad óptica, un disco duro óptico u otro medio para almacenar datos electrónicos. El eNB (u otra estación base) y UE (u otra estación móvil) también pueden incluir un componente transceptor, un componente contador, un componente de procesamiento y/o un componente de reloj o componente temporizador. Uno o más programas que puedan implementar o utilizar las diversas técnicas descritas en la presente memoria pueden utilizar una interfaz de programación de aplicaciones (API), controles reutilizables y similares. Tales programas pueden ser implementados en un lenguaje de programación de alto nivel, ya sea de procedimiento u orientado a objetos, para comunicarse con un sistema informático. Sin embargo, el programa o programas pueden ser implementados en lenguaje ensamblador o de máquina, si se desea. En cualquier caso, el lenguaje puede ser un lenguaje compilado o interpretado, y combinado con implementaciones de hardware.

Cada sistema informático incluye uno o más procesadores y/o memoria; los sistemas informáticos también pueden incluir diversos dispositivos de entrada y/o dispositivos de salida. El procesador puede incluir un dispositivo de uso general, tal como un microprocesador Intel©, AMD®, u otro disponible en el mercado. El procesador puede incluir un dispositivo de procesamiento de propósito especial, tal como ASIC, SoC, SiP FPGA, PAL, PLA, FPLA, PLD, u otro dispositivo personalizado o programable. La memoria puede incluir RAM estática, RAM dinámica, memoria flash, uno o más circuitos biestables, ROM, CD-ROM, DVD, disco, cinta, o magnético, óptico u otro medio de almacenamiento informático. El(los) dispositivo(s) de entrada puede(n) incluir un teclado, un ratón, una pantalla táctil, un lápiz óptico, una tableta, un micrófono, un sensor u otro hardware con el firmware y/o el software correspondiente. El(los) dispositivo(s) de salida puede(n) incluir un monitor u otra pantalla, una impresora, un sintetizador de voz o texto, un conmutador, una línea de señal, u otro hardware con el firmware y/o el software correspondiente.

Debe entenderse que muchas de las unidades funcionales descritas en esta memoria descriptiva pueden ser implementadas como uno o más componentes, que es un término usado para enfatizar más particularmente su independencia de implementación. Por ejemplo, un componente puede ser implementado como un circuito de hardware que comprende circuitos de integración a muy gran escala (VLSI) o puertas, o semiconductores disponibles en el mercado tales como chips lógicos, transistores u otros componentes discretos. También se puede implementar un componente en dispositivos de hardware programables tales como matrices de puertas programables en campo, una matriz lógica programable, dispositivos lógicos programables, o similares.

Los componentes también pueden implementarse en el software para su ejecución por diversos tipos de procesadores. Un componente identificado del código ejecutable puede comprender, por ejemplo, uno o más bloques físicos o lógicos de instrucciones informáticas que pueden, por ejemplo, organizarse como un objeto, un procedimiento o una función. Sin embargo, los ejecutables de un componente identificado no necesitan estar físicamente ubicados juntos, sino que pueden comprender instrucciones dispares almacenadas en diferentes ubicaciones que, cuando se unen lógicamente entre sí, comprenden el componente y conseguir el propósito indicado para el componente.

De hecho, un componente del código ejecutable puede ser una sola instrucción, o muchas instrucciones, y puede incluso distribuirse en varios segmentos de código diferentes, entre diferentes programas, y a través de varios dispositivos de memoria. De manera similar, los datos operativos pueden ser identificados e ilustrados en la presente dentro de los componentes, y se pueden incorporar en cualquier forma adecuada y organizarse dentro de cualquier tipo adecuado de estructura de datos. Los datos operativos pueden recogerse como un único conjunto de datos, o pueden distribuirse en diferentes localizaciones incluyendo diferentes dispositivos de almacenamiento, y puede existir, al menos parcialmente, simplemente como señales electrónicas en un sistema o red. Los componentes pueden ser pasivos o activos, incluyendo agentes operables para realizar las funciones deseadas.

Varios aspectos de las realizaciones descritas serán ilustrados como módulos o componentes de software. Tal como se utiliza en la presente, un módulo o componente de software puede incluir cualquier tipo de instrucciones de ordenador o código ejecutable por ordenador ubicado dentro de un dispositivo de memoria. Un módulo de software puede, por ejemplo, incluir uno o más bloques físicos o lógicos de instrucciones de ordenador, que pueden organizarse como una rutina, programa, objeto, componente, estructura de datos, etc., que realizan una o más tareas o implementan tipos de datos particulares. Se aprecia que un módulo de software puede implementarse en

hardware y/o firmware en lugar de o además de software. Uno o más de los módulos funcionales descritos en la presente memoria pueden ser separados en submódulos y/o combinados en un solo o menor número de módulos.

En ciertas realizaciones, un módulo de software particular puede incluir instrucciones dispares almacenadas en diferentes ubicaciones de un dispositivo de memoria, diferentes dispositivos de memoria, o diferentes ordenadores, que juntos implementan la funcionalidad descrita del módulo. De hecho, un módulo puede incluir una sola instrucción o muchas instrucciones y se pueden distribuir sobre varios segmentos de código diferentes, entre diferentes programas, y a través de varios dispositivos de memoria. Algunas realizaciones se pueden practicar en un entorno informático distribuido en donde las tareas se realizan por un dispositivo de procesamiento remoto enlazado a través de una red de comunicaciones. En un entorno informático distribuido, los módulos de software pueden estar situados en dispositivos de almacenamiento de memoria locales y/o remotos. Además, los datos que se vinculan o representan en un registro de base de datos pueden residir en el mismo dispositivo de memoria o en varios dispositivos de memoria, y pueden enlazarse entre sí en los campos de un registro de una base de datos de una red.

La referencia a lo largo de esta memoria descriptiva a "un ejemplo" significa que una característica particular, estructura o característica descrita en relación con el ejemplo, se incluye en al menos una realización de la presente invención. Así, las apariciones de la frase "en un ejemplo" en diversos lugares a lo largo de esta memoria no se refieren necesariamente a la misma realización.

Tal como se utiliza en la presente, una pluralidad de artículos, elementos estructurales, elementos de composición y/o materiales pueden presentarse en una lista común por conveniencia. Sin embargo, estas listas deben interpretarse como si cada miembro de la lista se identificara individualmente como un miembro separado y único. De esta manera, ningún miembro individual de esa lista debe interpretarse como un equivalente de facto de otro miembro de la misma lista basado únicamente en su presentación en un grupo común sin indicaciones en contrario. Además, se pueden hacer referencia a diversas realizaciones y ejemplos de la presente invención junto con alternativas para sus diversos componentes. Se entiende que tales realizaciones, ejemplos y alternativas no deben interpretarse como equivalentes entre sí, sino que deben considerarse como representaciones independientes y autónomas de la presente invención.

Se debe reconocer que los sistemas descritos en la presente memoria incluyen descripciones de realizaciones específicas. Estas realizaciones se pueden combinar en sistemas individuales, parcialmente combinadas en otros sistemas, divididas en múltiples sistemas o divididas o combinadas de otras maneras. Además, se contempla que los parámetros/atributos/aspectos/etc. de una realización pueden utilizarse en otra realización. Los parámetros/atributos/aspectos/etc. se describen simplemente en una o más realizaciones para mayor claridad y se reconoce que los parámetros/atributos/aspectos/etc. pueden combinarse o sustituirse por parámetros/atributos/etc. de otra realización a menos que se indique específicamente en la presente.

REIVINDICACIONES

1. Un aparato para uso en un equipo (102) de usuario, en el que el aparato se caracteriza por que está configurado para:

encapsular un mensaje de vehículo a dispositivo que no sea de protocolo de Internet, no IP, como unidad de datos de servicio, SDU, en un protocolo de convergencia de datos en paquetes, PDCP, unidad de datos de protocolo, PDU, que incluya una unidad de datos de servicio, SDU, campo (202) de tipo, en el que el mensaje de vehículo a dispositivo no IP sea un mensaje compatible con el protocolo IEEE 1609;

establecer el campo (202) de tipo SDU para indicar que el mensaje de vehículo a dispositivo no IP es de tipo SDU no IP; y

provocar la transmisión de la PDCP PDU a otro equipo (104) de usuario a través de una interfaz inalámbrica entre el equipo (102) de usuario y el otro equipo (104) de usuario.

2. El aparato de la reivindicación 1, en el que el mensaje no IP de vehículo a dispositivo es un acceso inalámbrico en entornos vehiculares, WAVE, mensaje.

3. El aparato de la reivindicación 2, en el que el mensaje WAVE es como protocolo de mensaje corto WAVE, WSMP, mensaje.

4. El aparato de la reivindicación 1, en el que el aparato está configurado además para establecer un enlace seguro con el otro equipo (102) de usuario utilizando una interfaz PC5.

5. El aparato de la reivindicación 4, en el que el aparato comprende además un identificador de capa 2 del otro equipo (104) de usuario a la PDCP PDU.

6. Un aparato para uso en un equipo (104) de usuario, el aparato caracterizado por que está configurado para:

recibir un protocolo de convergencia de datos en paquetes, PDCP, unidad de datos de protocolo, PDU, de otro equipo de usuario (102) a través de una interfaz inalámbrica entre el equipo de usuario (104) y el otro equipo de usuario (102);

detectar un campo de tipo (202) de una unidad de datos de servicio PDCP, SDU, dentro de la PDCP PDU, lo que indica que un mensaje de vehículo a dispositivo sin protocolo de Internet, sin IP, que forma la PDCP SDU no es de tipo IP;

extraer la PDCP SDU de la PDCP PDU; y

extraer el mensaje de vehículo a dispositivo no IP del PDCP SDU, en el que el mensaje de vehículo a dispositivo no IP es un mensaje compatible con el protocolo IEEE 1609.

7. El aparato de la reivindicación 6, en el que el tipo de mensaje no IP de vehículo a dispositivo es un acceso inalámbrico en entornos vehiculares, WAVE, mensaje.

8. El aparato de la reivindicación 7, en el que el mensaje WAVE es un protocolo de mensaje corto WAVE, WSMP, mensaje.

9. Un método de transmisión de un mensaje de vehículo a dispositivo sin protocolo de Internet, no IP, el método se caracteriza por que comprende:

encapsular un mensaje de vehículo a dispositivo que no sea de protocolo de Internet, no IP, como unidad de datos de servicio, SDU, en un protocolo de convergencia de datos en paquetes, PDCP, unidad de datos de protocolo, PDU, que incluya un campo (202) de tipo SDU, en el que el mensaje de vehículo a dispositivo no IP sea un mensaje compatible con el protocolo IEEE 1609;

establecer el campo (202) de tipo SDU para indicar que el mensaje de vehículo a dispositivo no IP es de tipo SDU no IP; y

provocar la transmisión de la PDCP PDU a otro equipo (104) de usuario a través de una interfaz inalámbrica entre el equipo (102) de usuario y el otro equipo (104) de usuario.

10. El aparato de la reivindicación 9, en el que el tipo de mensaje no IP de vehículo a dispositivo es un acceso inalámbrico en entornos vehiculares, WAVE, mensaje.

11. El método de la reivindicación 10, en el que el mensaje WAVE es un protocolo de mensaje corto WAVE, WSMP, mensaje.

12. Un método para recibir un mensaje de vehículo a dispositivo sin protocolo de Internet, no IP, el método se caracteriza por que comprende:

recibir de un protocolo de convergencia de datos en paquetes, PDCP, unidad de datos de protocolo, PDU, de otro equipo de usuario (102) a través de una interfaz inalámbrica entre el equipo de usuario (104) y el otro equipo de usuario (102);

detectar de un campo de tipo (202) de una unidad de datos de servicio PDCP, SDU, dentro de la PDCP PDU, lo que indica que un mensaje de vehículo a dispositivo sin protocolo de Internet, sin IP, que forma la PDCP SDU no es de tipo IP;

extraer de la PDCP SDU de la PDCP PDU; y

extraer del mensaje de vehículo a dispositivo no IP del PDCP SDU, en el que el mensaje de vehículo a dispositivo no IP es un mensaje compatible con el protocolo IEEE 1609.

13. El método de la reivindicación 12, en el que el tipo de mensaje no IP de vehículo a dispositivo es un acceso inalámbrico en entornos vehiculares, WAVE, mensaje.

14. El método de la reivindicación 13, en el que el mensaje WAVE es un protocolo de mensaje corto WAVE, WSMP, mensaje.

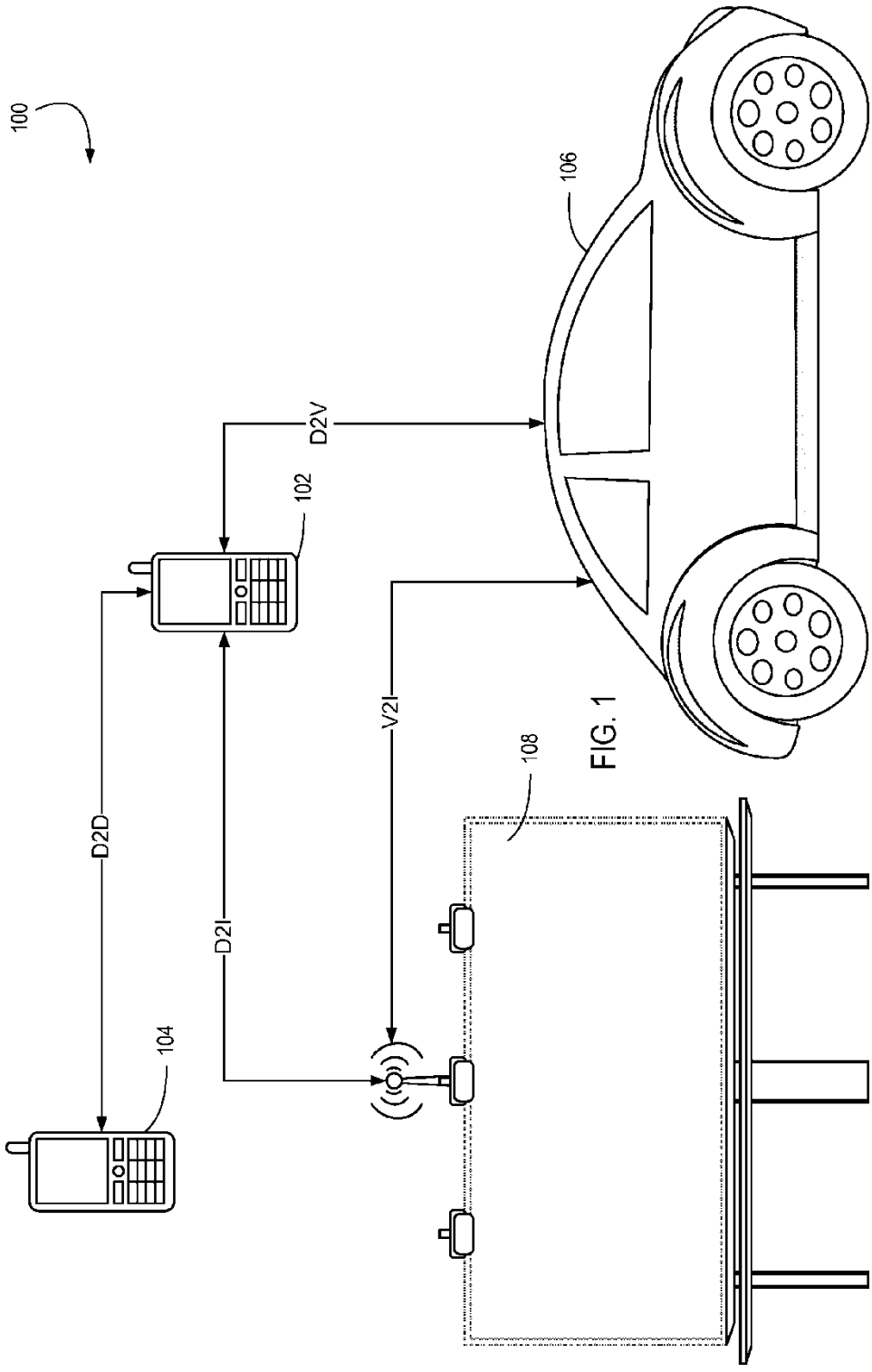

FIG. 1

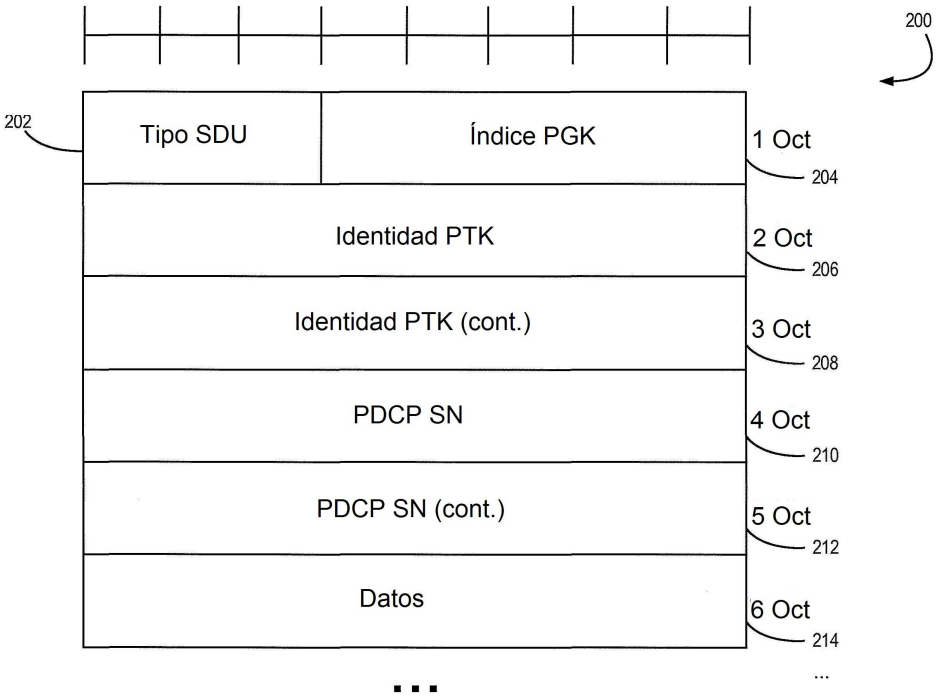
200
202
Tipo SDU
Índice PGK
1 Oct
204
Identidad PTK
2 Oct
206
Identidad PTK (cont.)
3 Oct
208
PDCP SN
4 Oct
210
PDCP SN (cont.)
5 Oct
212
Datos
6 Oct
214
...

FIG. 2

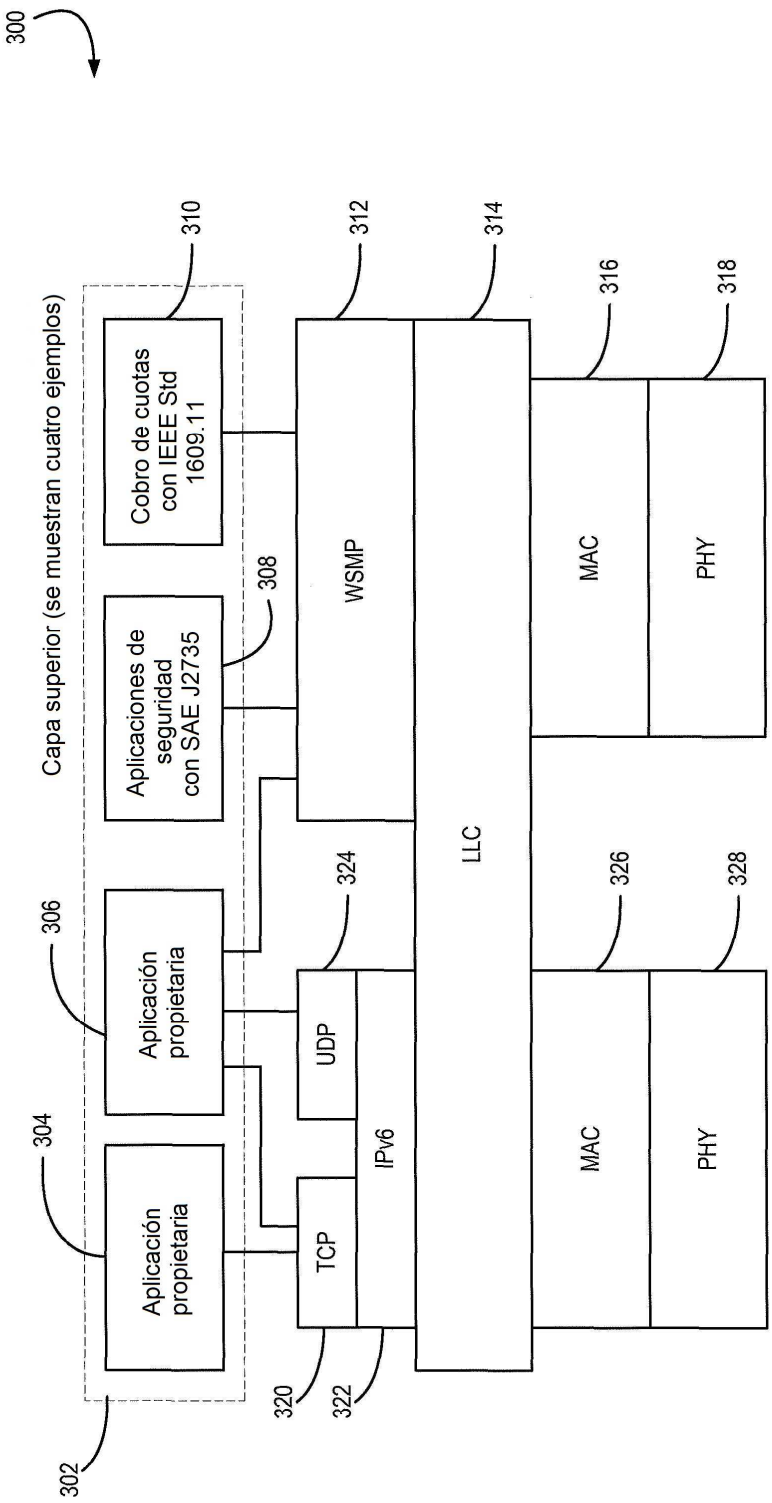
300
Capa superior (se muestran cuatro ejemplos)
Cobro de cuotas con IEEE Std 1609.11
Aplicaciones de seguridad con SAE J2735
Aplicación propietaria
Aplicación propietaria
WSMP
LLC
MAC
PHY
MAC
PHY
UDP
TCP
IPv6
302
304
306
308
310
312
314
316
318
320
322
324
326
328

FIG. 3

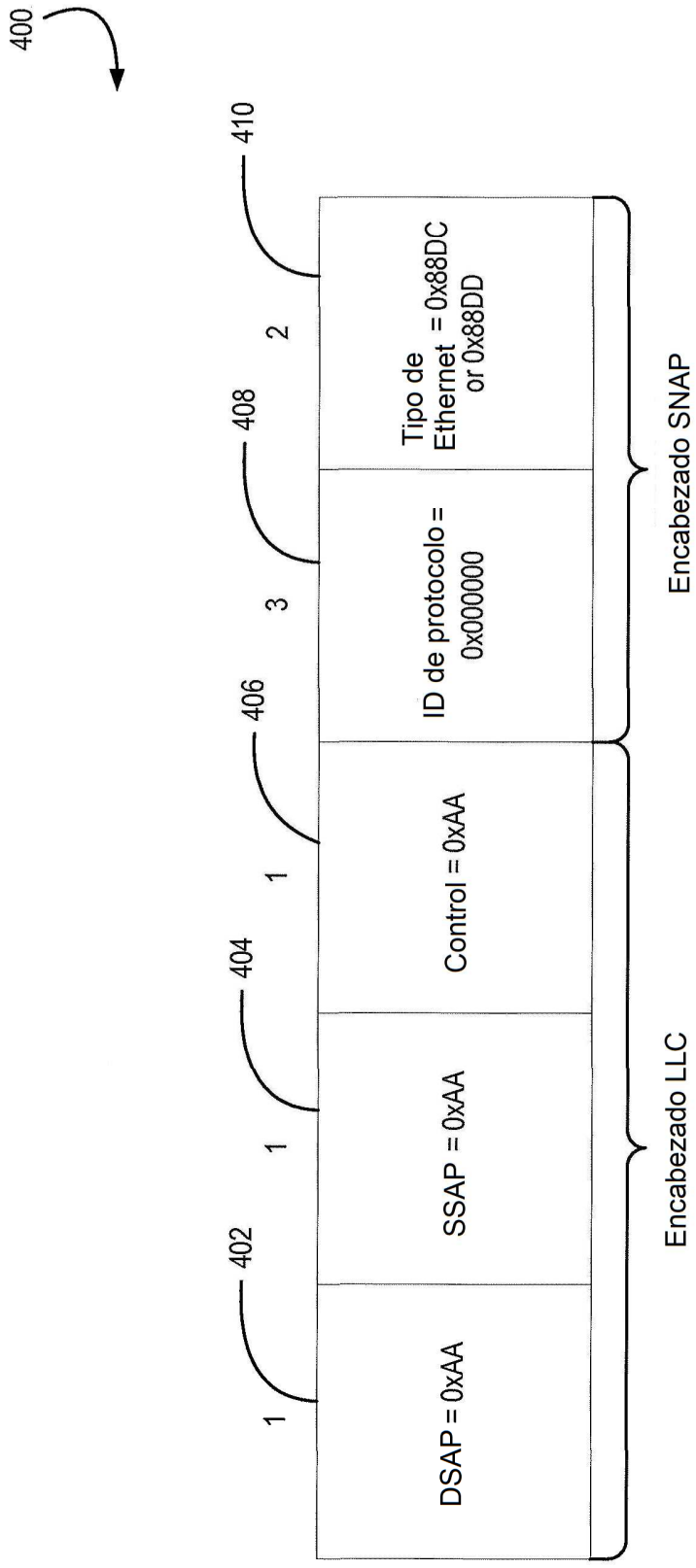
400
402
404
406
408
410
1
1
1
3
2
DSAP = 0xAA
SSAP = 0xAA
Control = 0xAA
ID de protocolo = 0x000000
Tipo de Ethernet = 0x88DC or 0x88DD
Encabezado LLC
Encabezado SNAP

FIG. 4

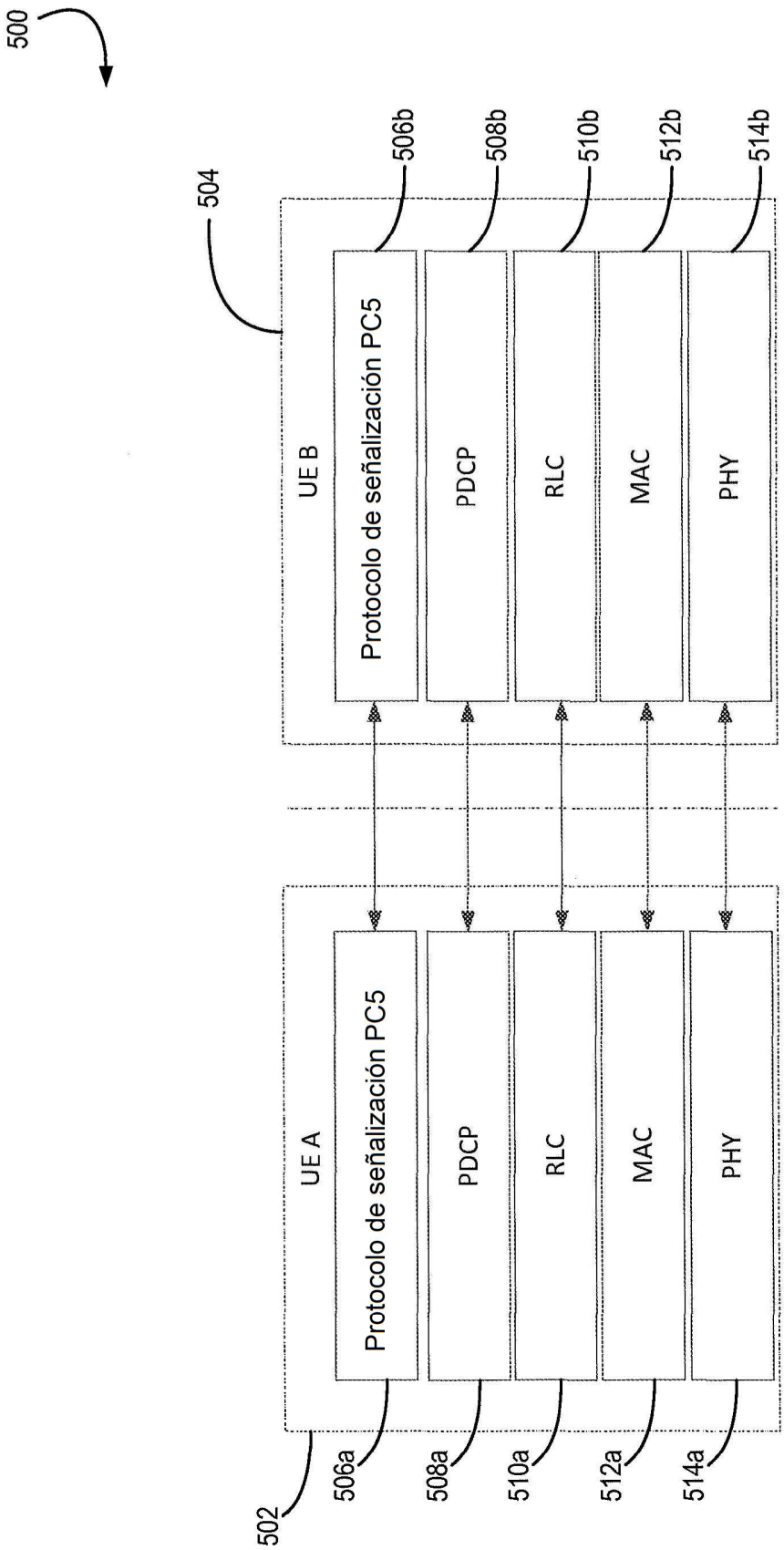
500
504
506b
508b
510b
512b
514b
UE B
Protocolo de señalización PC5
PDCP
RLC
MAC
PHY
UE A
Protocolo de señalización PC5
PDCP
RLC
MAC
PHY
502
506a
508a
510a
512a
514a
Pila de protocolo de señalización PC5

FIG. 5

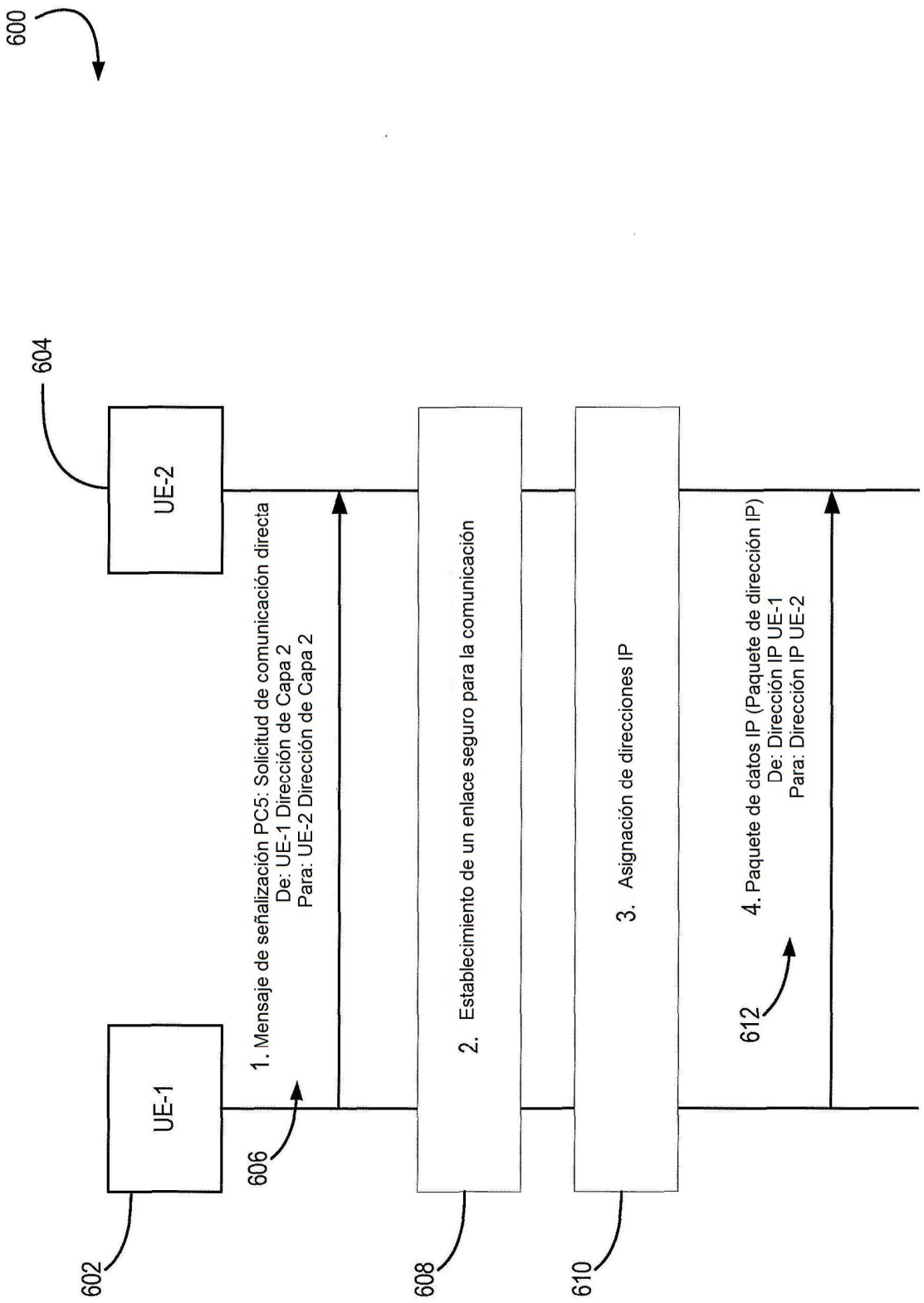
600
604
UE-2
UE-1
602
606
608
610
612
1. Mensaje de señalización PC5: Solicitud de comunicación directa
De: UE-1 Dirección de Capa 2
Para: UE-2 Dirección de Capa 2
2. Establecimiento de un enlace seguro para la comunicación
3. Asignación de direcciones IP
4. Paquete de datos IP (Paquete de dirección IP)
De: Dirección IP UE-1
Para: Dirección IP UE-2

FIG. 6

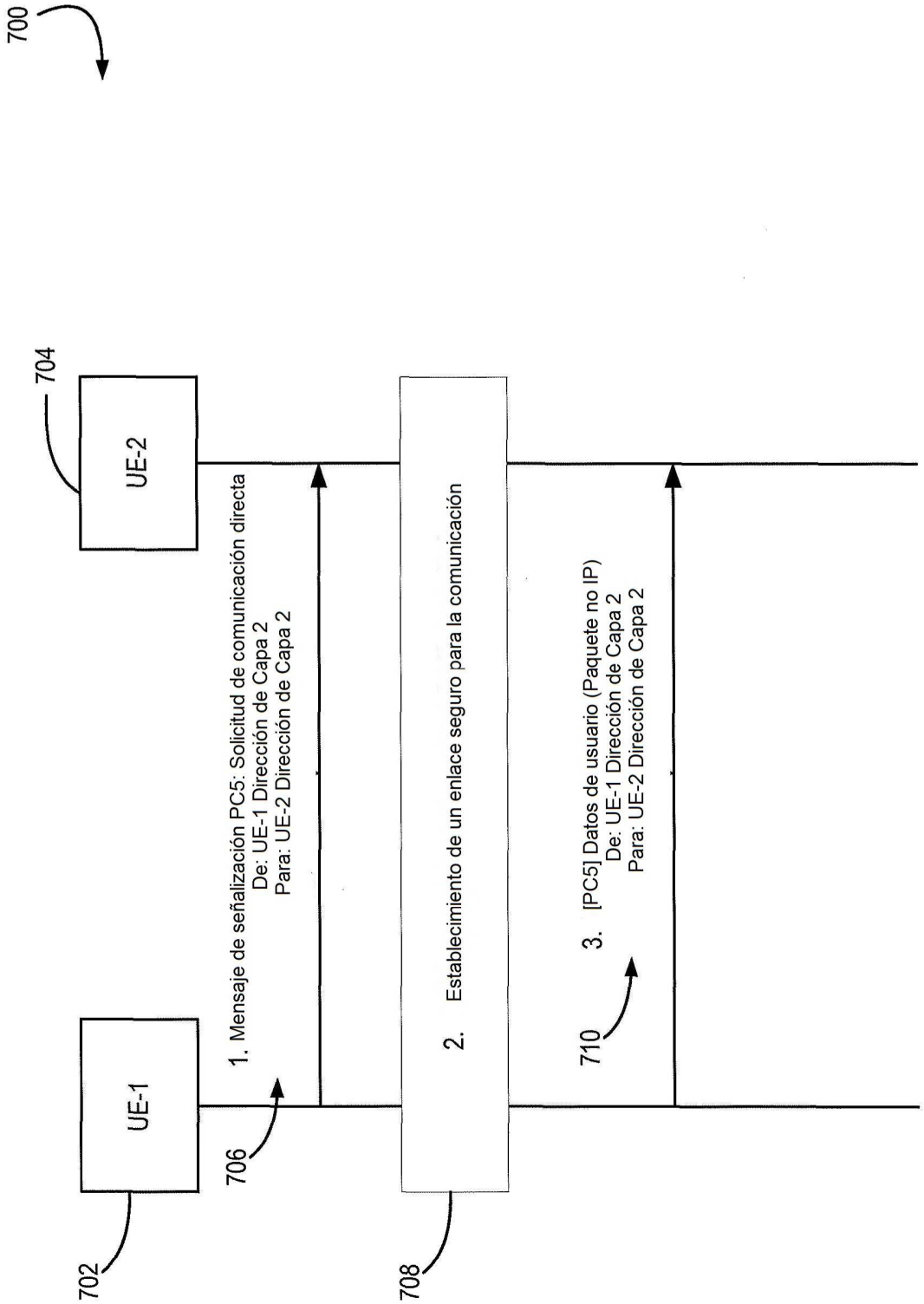
700
704
UE-2
UE-1
1. Mensaje de señalización PC5: Solicitud de comunicación directa
De: UE-1 Dirección de Capa 2
Para: UE-2 Dirección de Capa 2
2. Establecimiento de un enlace seguro para la comunicación
3. [PC5] Datos de usuario (Paquete no IP)
De: UE-1 Dirección de Capa 2
Para: UE-2 Dirección de Capa 2
710
706
702
708

FIG. 7

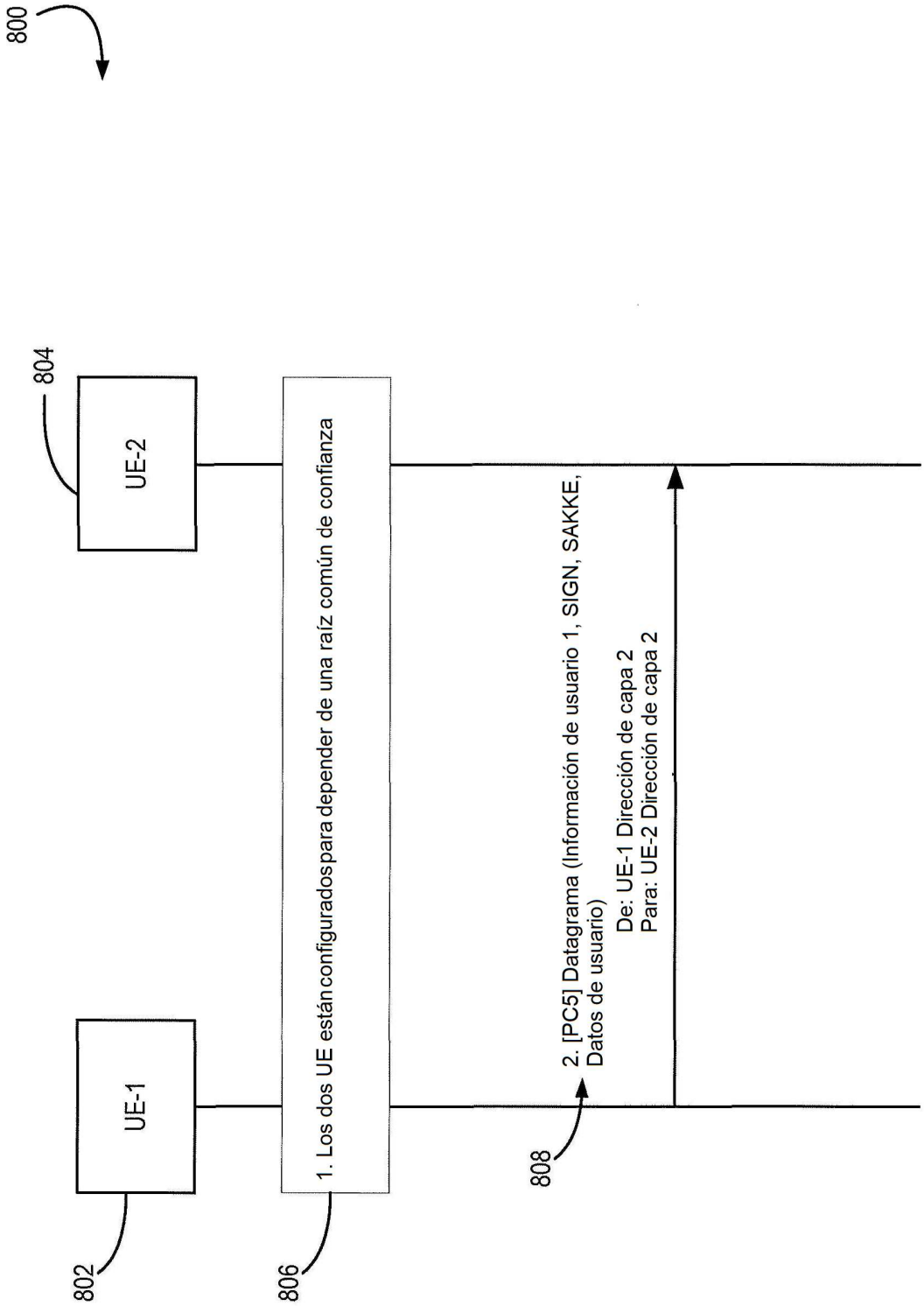
800
804
UE-2
1. Los dos UE están configurados para depender de una raíz común de confianza
UE-1
2. [PC5] Datagrama (Información de usuario 1, SIGN, SAKKE, Datos de usuario)
De: UE-1 Dirección de capa 2
Para: UE-2 Dirección de capa 2
802
806
808

FIG. 8

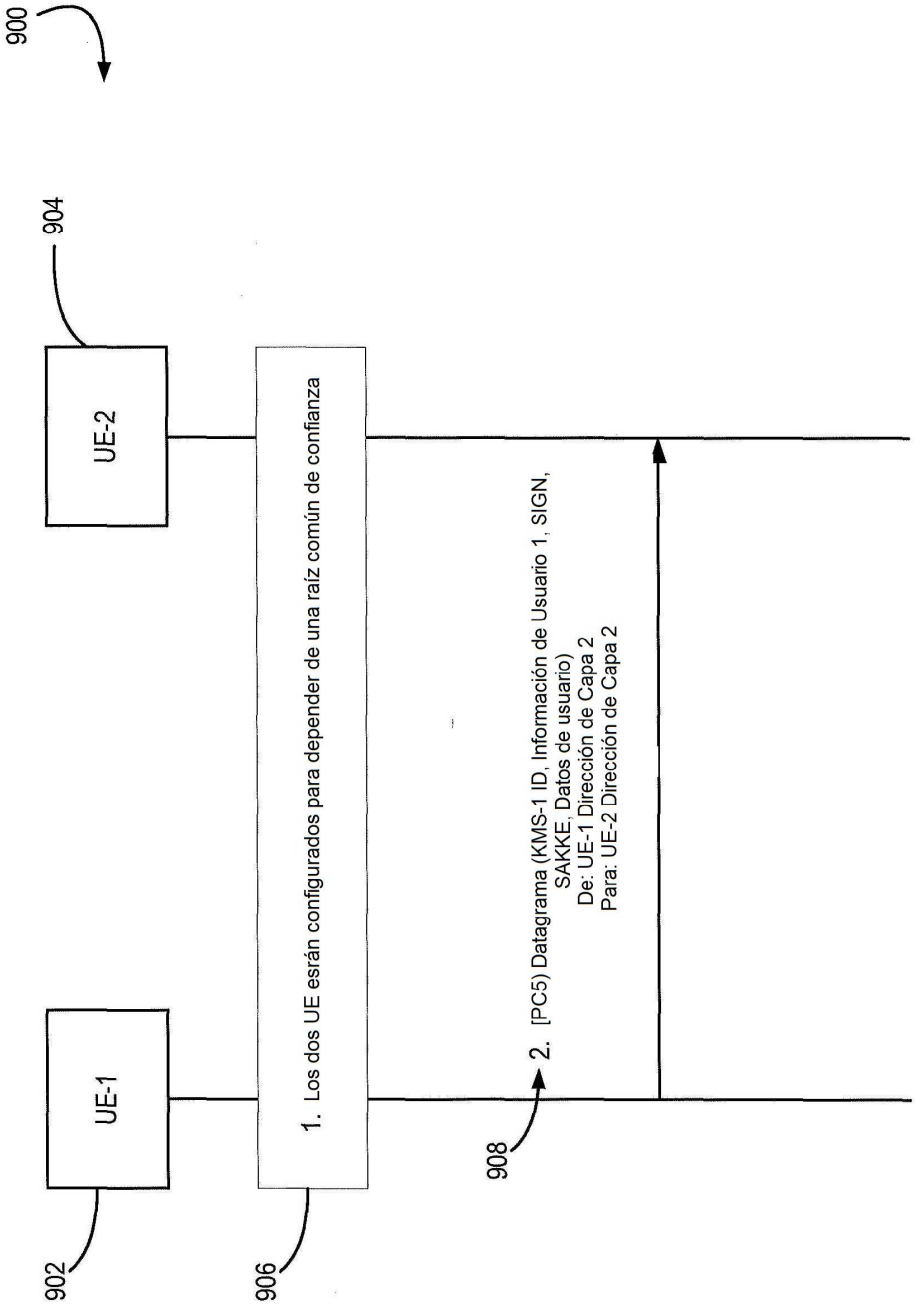
900
904
UE-2
1. Los dos UE serán configurados para depender de una raíz común de confianza
2. [PC5) Datagrama (KMS-1 ID, Información de Usuario 1, SIGN, SAKKE, Datos de usuario)
De: UE-1 Dirección de Capa 2
Para: UE-2 Dirección de Capa 2
908
UE-1
902
906

FIG. 9

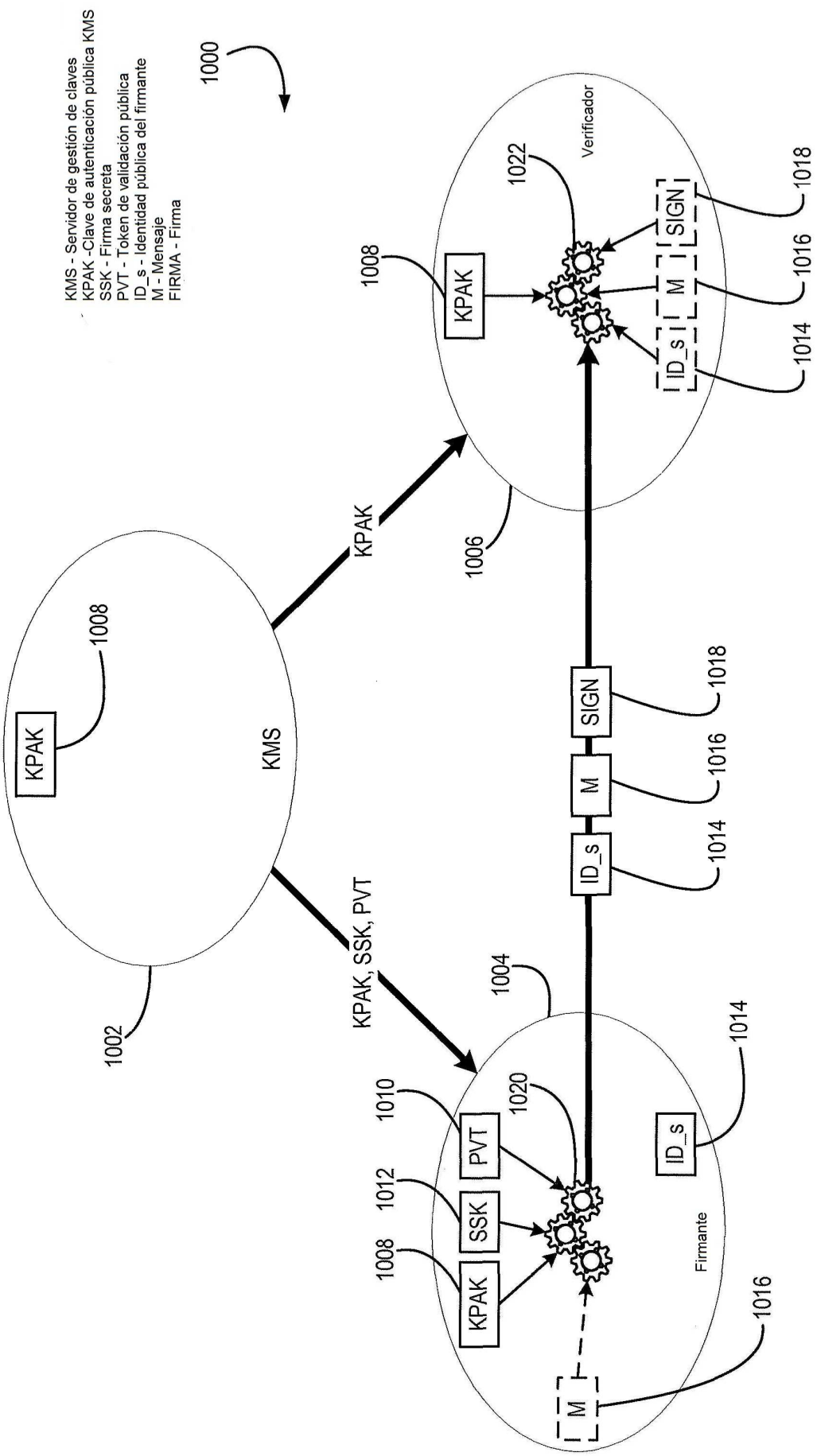
KMS - Servidor de gestión de claves
KPAK -Clave de autenticación pública KMS
SSK - Firma secreta
PVT - Token de validación pública
ID_s - Identidad pública del firmante
M - Mensaje
FIRMA - Firma
1000
KMS
1002
KPAK
1008
KPAK, SSK, PVT
KPAK
1006
Verificador
1022
1008
KPAK
ID_s
M
SIGN
1014
1016
1018
1004
Firmante
1008
KPAK
1012
SSK
1010
PVT
1020
ID_s
1014
M
1016

FIG. 10

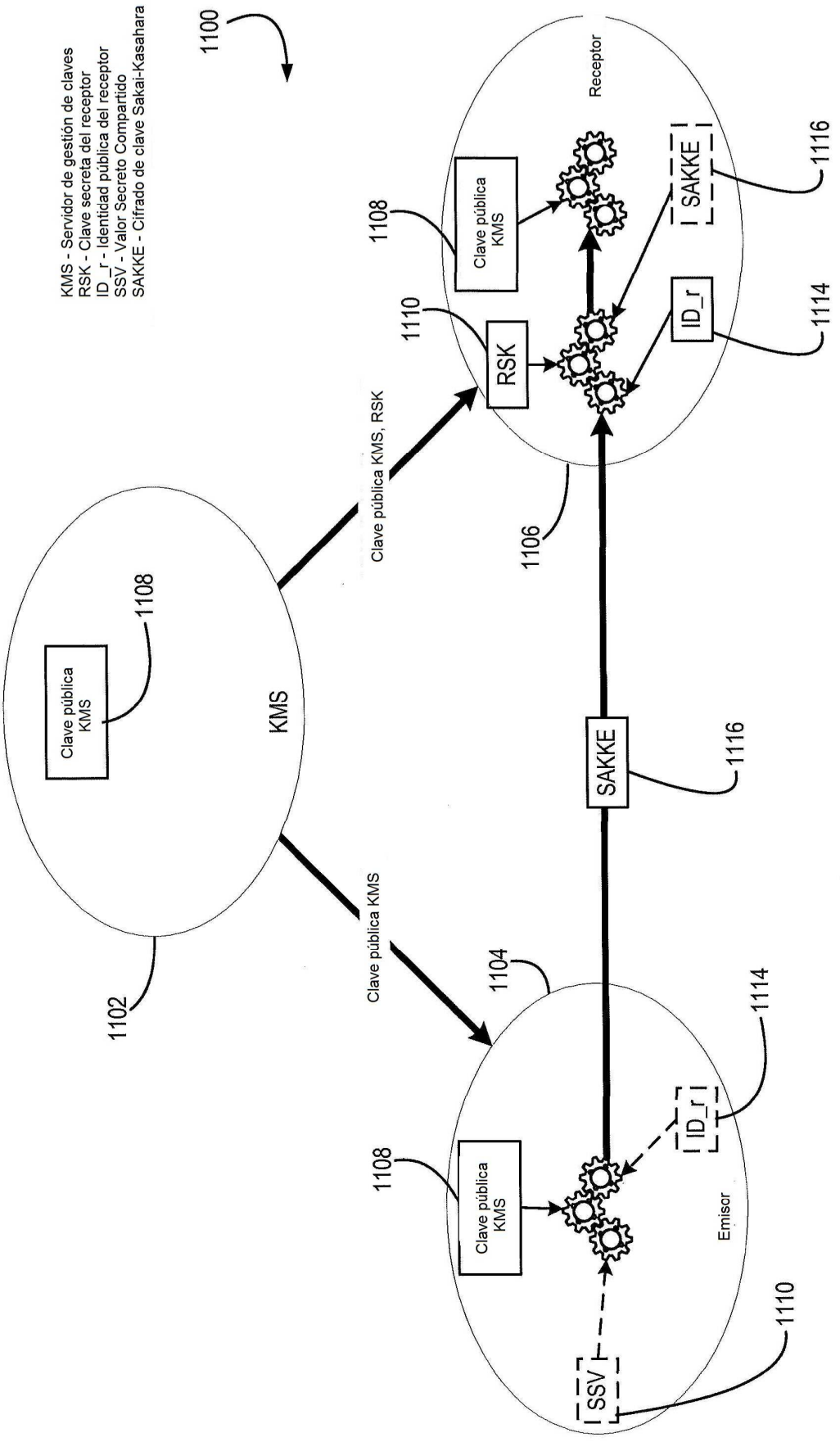
KMS - Servidor de gestión de claves
RSK - Clave secreta del receptor
ID_r - Identidad pública del receptor
SSV - Valor Secreto Compartido
SAKKE - Cifrado de clave Sakai-Kasahara
1100
KMS
1102
Clave pública KMS
1108
Clave pública KMS
Clave pública KMS, RSK
Receptor
1106
Clave pública KMS
1108
RSK
1110
SAKKE
1116
ID_r
1114
SAKKE
1116
Emisor
1104
Clave pública KMS
1108
ID_r
1114
SSV
1110

FIG. 11

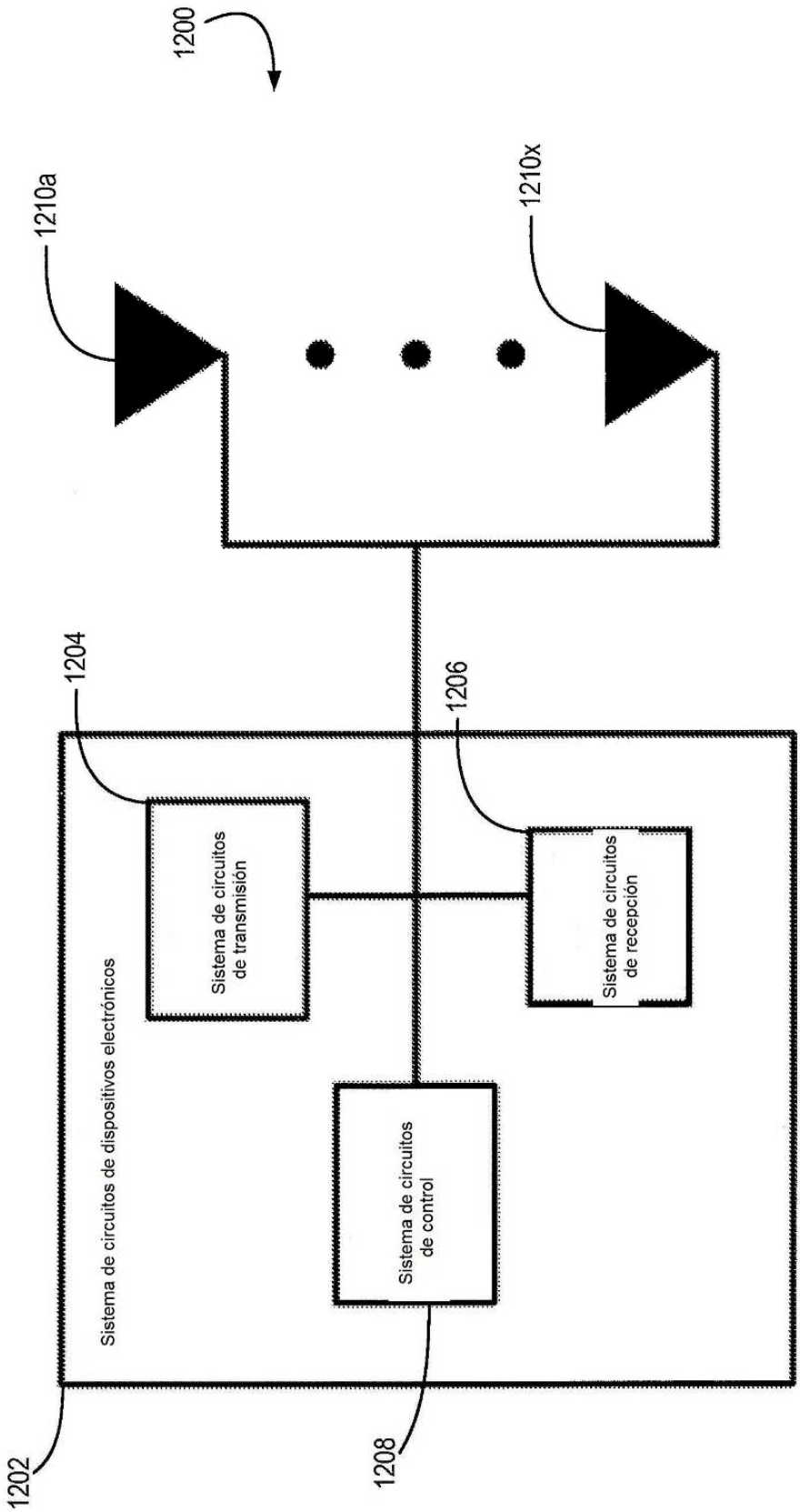
1200
1210a
1210x
1204
1206
Sistema de circuitos de transmisión
Sistema de circuitos de recepción
Sistema de circuitos de dispositivos electrónicos
Sistema de circuitos de control
1202
1208

FIG. 12

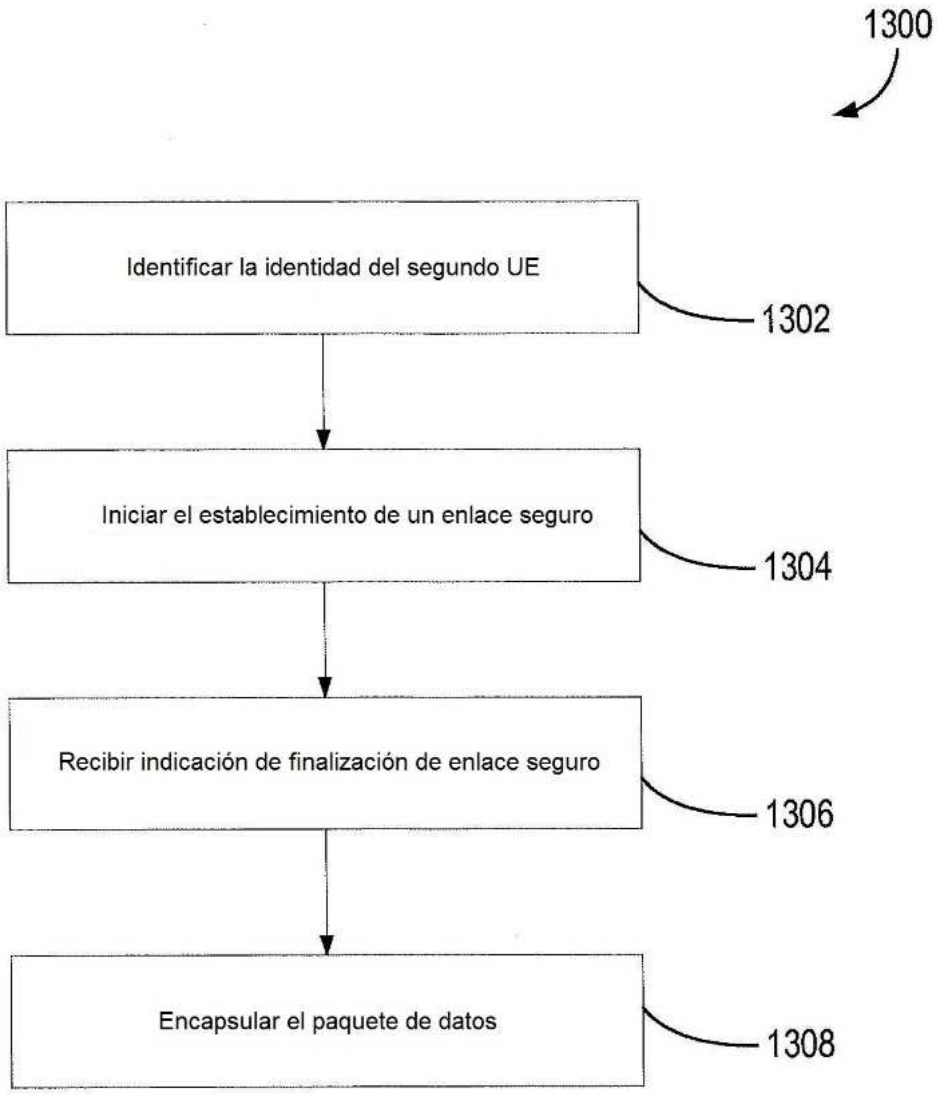
1300
Identificar la identidad del segundo UE
1302
Iniciar el establecimiento de un enlace seguro
1304
Recibir indicación de finalización de enlace seguro
1306
Encapsular el paquete de datos
1308

FIG. 13

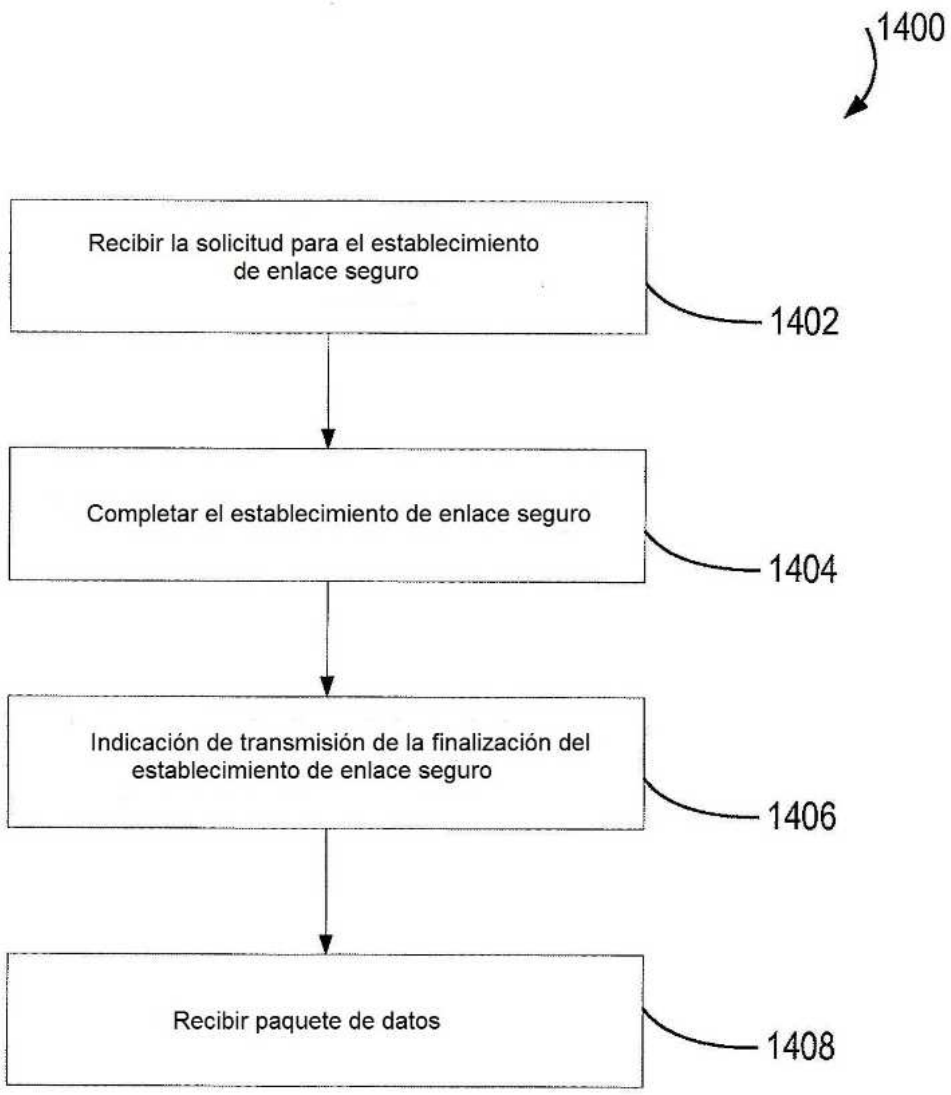
1400
Recibir la solicitud para el establecimiento de enlace seguro
1402
Completar el establecimiento de enlace seguro
1404
Indicación de transmisión de la finalización del establecimiento de enlace seguro
1406
Recibir paquete de datos
1408

FIG. 14

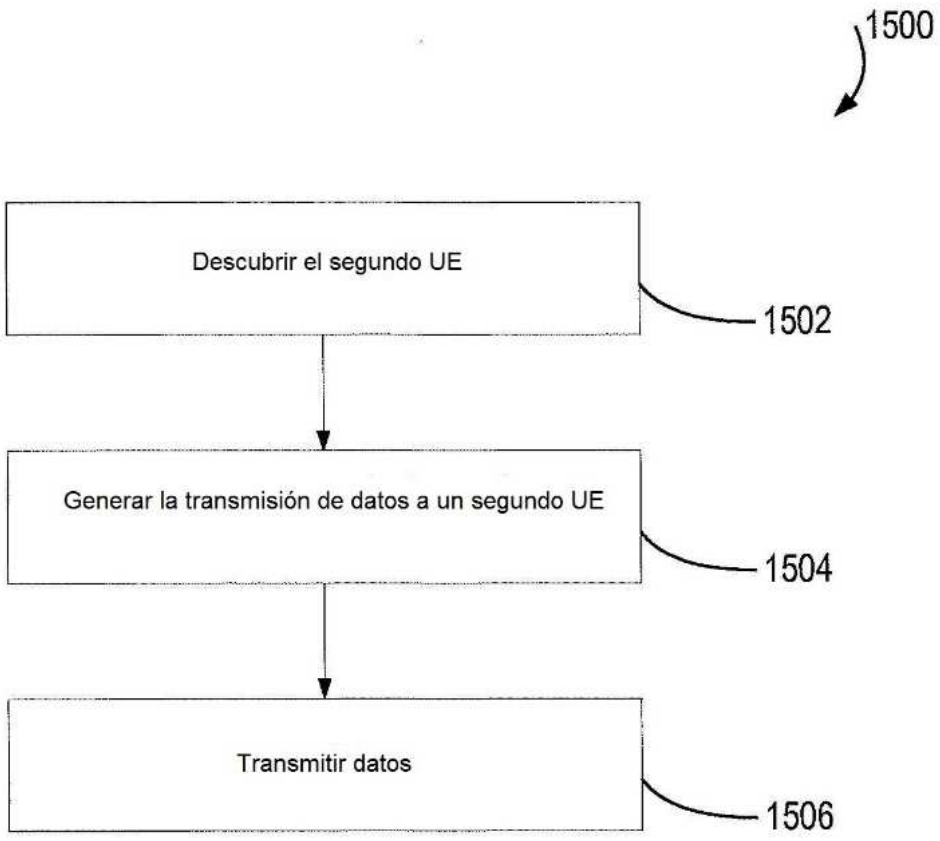
1500
Descubrir el segundo UE
1502
Generar la transmisión de datos a un segundo UE
1504
Transmitir datos
1506

FIG. 15

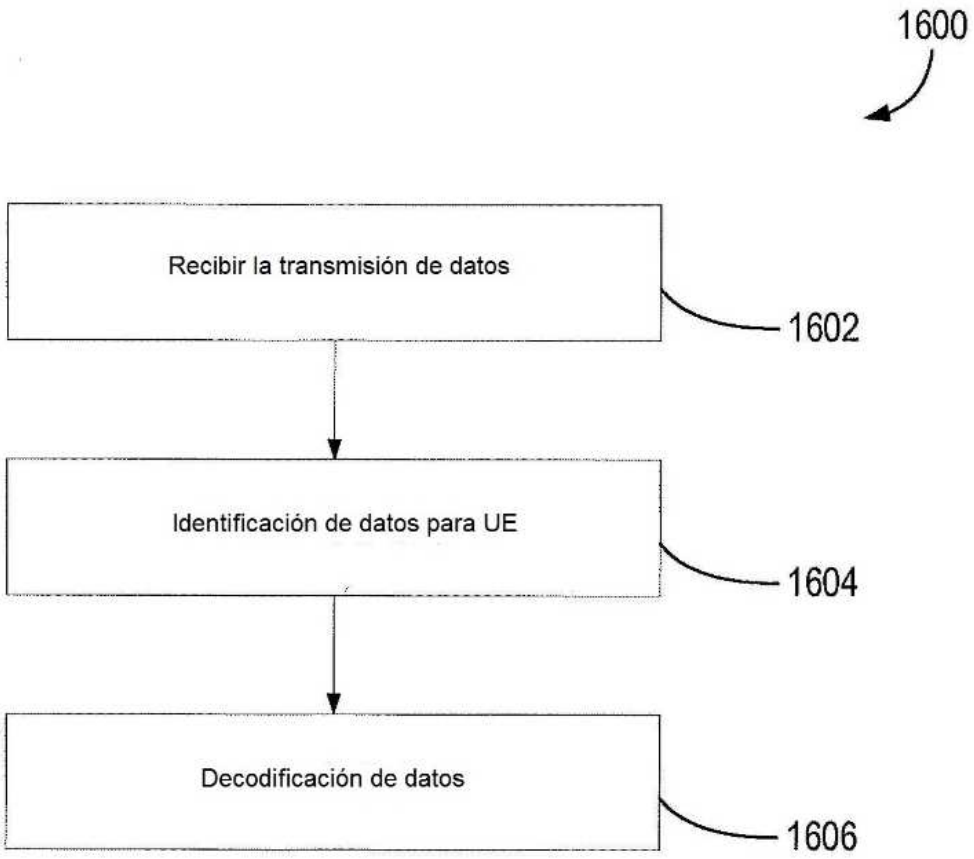
1600
Recibir la transmisión de datos
1602
Identificación de datos para UE
1604
Decodificación de datos
1606

FIG. 16

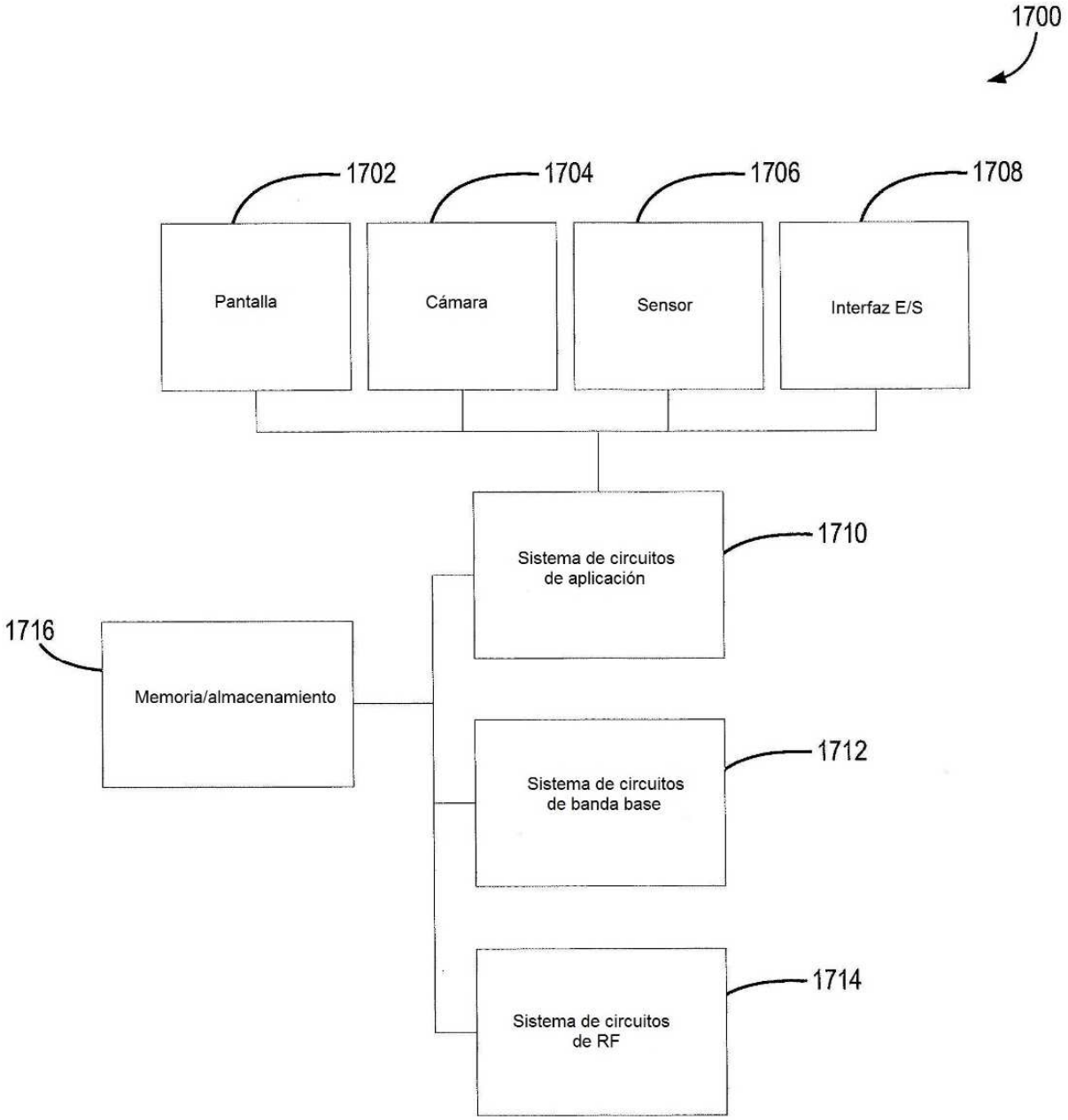
1700
1702
1704
1706
1708
Pantalla
Cámara
Sensor
Interfaz E/S
Sistema de circuitos de aplicación
1710
1716
Memoria/almacenamiento
Sistema de circuitos de banda base
1712
Sistema de circuitos de RF
1714

FIG. 17

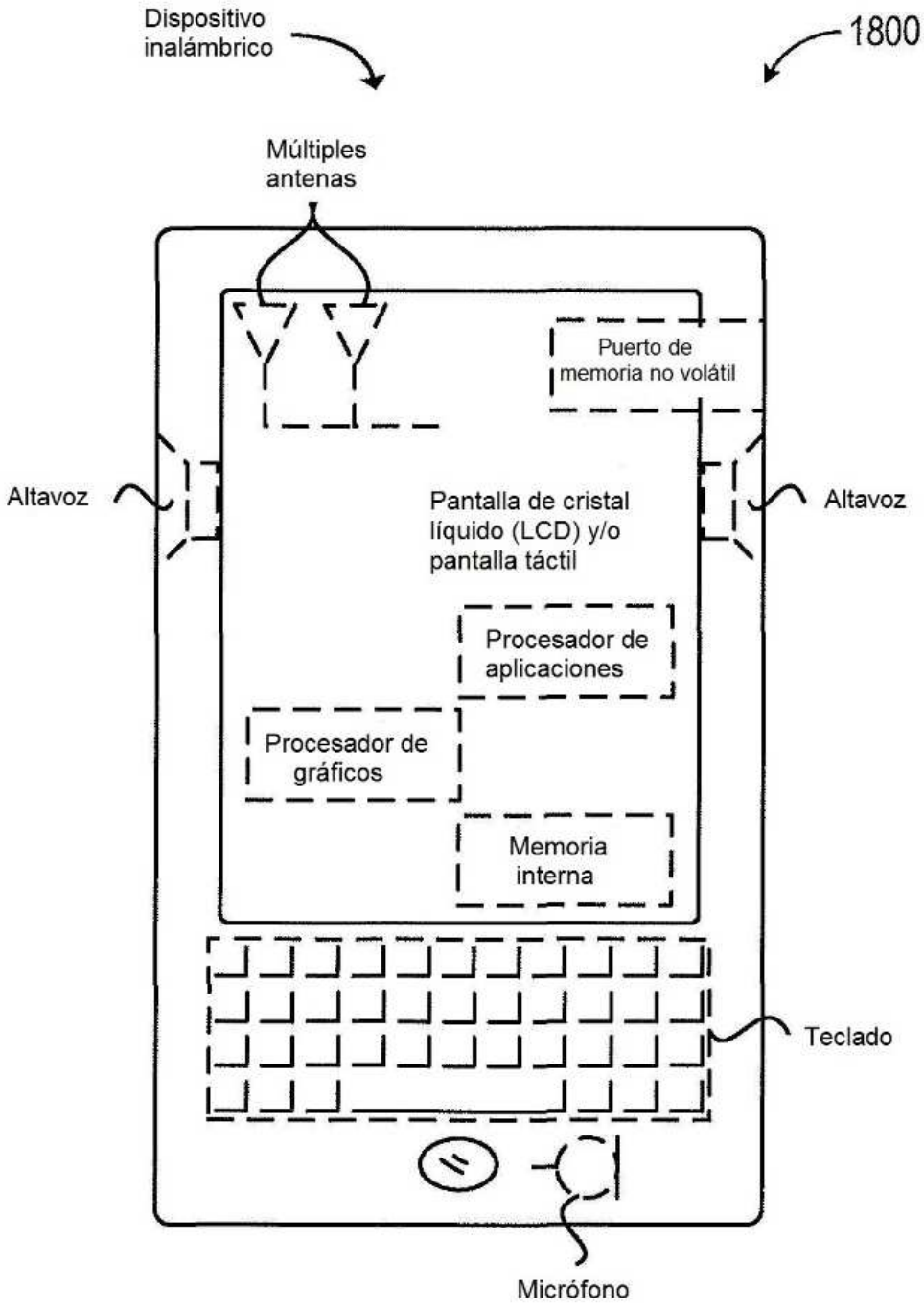
Dispositivo inalámbrico
1800
Múltiples antenas
Puerto de memoria no volátil
Altavoz
Altavoz
Pantalla de cristal líquido (LCD) y/o pantalla táctil
Procesador de aplicaciones
Procesador de gráficos
Memoria interna
Teclado
Micrófono

FIG. 18

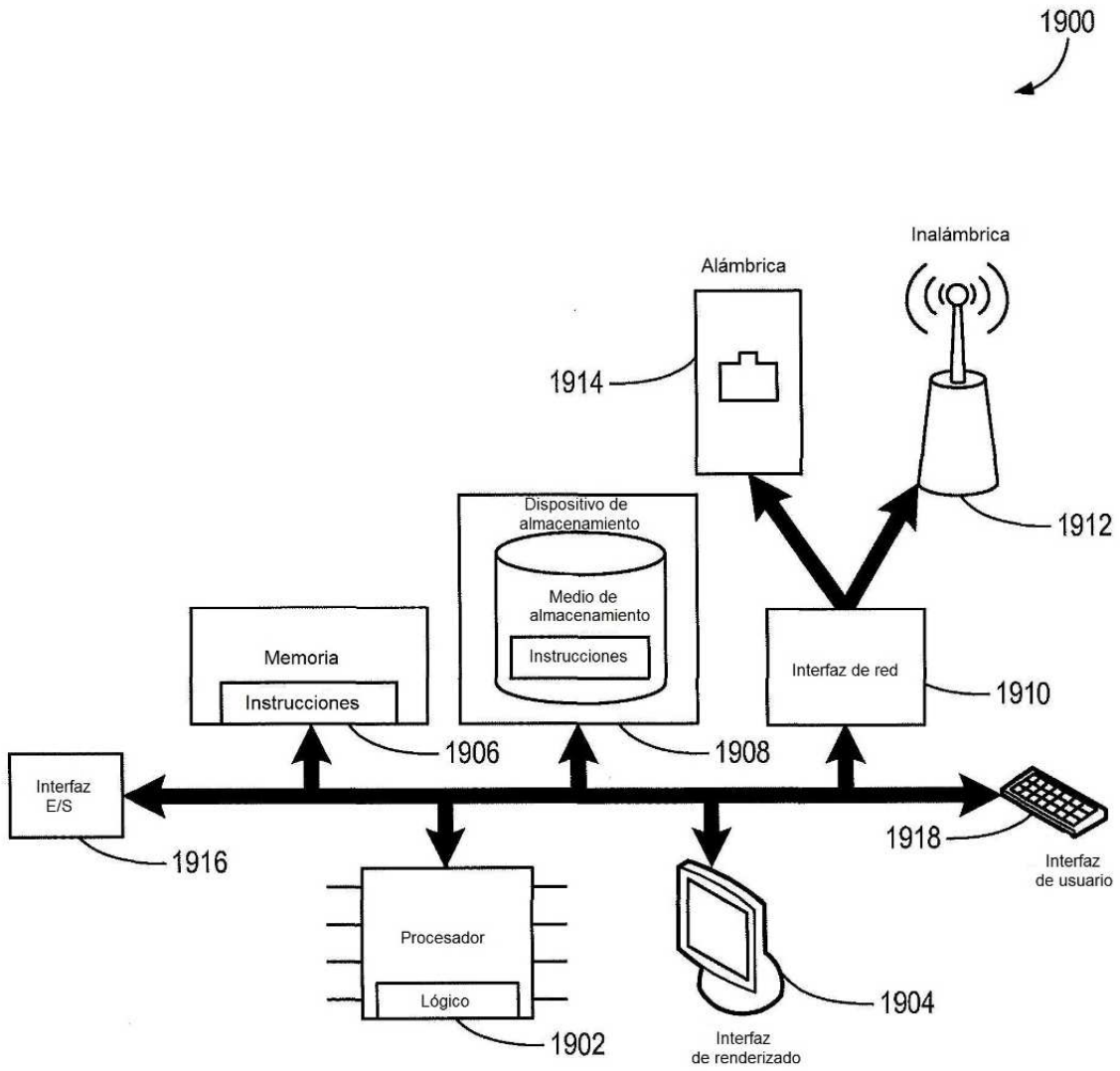
1900
Inalámbrica
Alámbrica
1914
1912
Dispositivo de almacenamiento
Medio de almacenamiento
Instrucciones
Memoria
Instrucciones
Interfaz de red
1910
1906
1908
Interfaz E/S
1916
1918
Interfaz de usuario
Procesador
Lógico
1902
1904
Interfaz de renderizado

FIG. 19