

REDES PERSONALES DE INTERNET DE LAS COSAS

REFERENCIA CRUZADA A SOLICITUDES RELACIONADAS

- 5 La presente solicitud reivindica prioridad a la solicitud provisional de los EE. UU. núm. 63/304.487, presentada el 28 de enero de 2022, titulada "PERSONAL INTERNET-OF-THINGS NETWORKS", la que se incorpora en la presente descripción como referencia en su totalidad.

ANTECEDENTES

10

Las redes de comunicación inalámbrica proporcionan plataformas de comunicación y servicios de telecomunicaciones integrados a dispositivos de usuario inalámbricos. Los servicios de telecomunicaciones ilustrativos incluyen telefonía, datos (p. ej., voz, audio, y/o datos de video), mensajería, acceso a Internet, y/u otros servicios. Las redes de comunicación inalámbrica

15 tienen nodos de acceso inalámbrico que intercambian señales inalámbricas con los dispositivos de usuario inalámbricos usando protocolos de red inalámbrica, tales como los protocolos descritos en diversas normas de telecomunicaciones promulgadas por el Proyecto Asociación de Tercera Generación (3GPP, en inglés). Las redes de comunicación inalámbrica ilustrativas incluyen redes de acceso múltiple por división de código (CDMA, en inglés), redes

20 de acceso múltiple por división de tiempo (TDMA, en inglés), redes de acceso múltiple por división de frecuencia (FDMA, en inglés), redes de acceso múltiple por división de frecuencia ortogonal (OFDMA, en inglés), evolución a largo plazo (LTE, en inglés) y nueva radio de quinta generación (5G NR, en inglés). Las redes de comunicación inalámbrica facilitan el servicio de banda ancha móvil usando tecnologías tales como OFDM, salida múltiple entrada múltiple

25 (MIMO), codificación de canales avanzada, MIMO masiva, formación de haces, y/u otras características.

SUMARIO

Una de las características que está desarrollando el Proyecto de Asociación de Tercera Generación (3GPP) es una red personal de Internet de las cosas (IoT, en inglés) (PIN, en inglés). Una PIN puede operarse en cooperación con una red móvil terrestre pública doméstica (PLMN, en inglés) proporcionada por un operador de red móvil (MNO, en inglés). Sin embargo, las PIN siguen en desarrollo y actualmente existen muchos desafíos no abordados que enfrenta la adopción de PIN.

En la presente descripción se describen soluciones que abordan muchos de los desafíos abiertos que enfrenta la adopción de PIN. Entre otras cosas, esta descripción describe atributos de PIN, aspectos arquitectónicos de PIN, configuraciones para la autorización de PEGC/PEMC, configuraciones para la operación de PIN en conexión con una red asociada, identificadores para el establecimiento de PIN y parámetros de políticas, procedimientos para la notificación y suministro de parámetros, establecimiento de PIN con políticas suministradas previamente o con políticas dinámicas, y establecimiento de PIN dinámica iniciado por el UE. Esta descripción también describe métodos y sistemas para implementar las soluciones descritas.

De acuerdo con un aspecto de la presente descripción, se describe un método que debe realizar un equipo de usuario (UE, en inglés). El método implica generar una solicitud de registro que incluye una capacidad del UE para servir como una puerta de enlace para una red personal de Internet de las cosas (PIN); enviar la solicitud de registro a una estación base que sirve al UE; recibir, de la estación base, un mensaje de aceptación de registro que incluye una autorización de puerta de enlace de PIN; e iniciar el establecimiento de PIN con al menos otro dispositivo, donde el UE sirve como puerta de enlace de PIN a la estación base.

Otras versiones incluyen sistemas, aparatos y programas informáticos correspondientes para realizar las acciones de los métodos definidos por instrucciones codificadas en dispositivos de

almacenamiento legibles por computadora. Estas y otras versiones pueden incluir opcionalmente una o más de las siguientes características.

En algunas implementaciones, la solicitud de registro incluye además uno o más atributos de PIN.

- 5 En algunas implementaciones, uno o más atributos de PIN incluyen al menos uno de: una clase de PIN, un alcance de tráfico de PIN que proporciona una ubicación de tráfico de PIN, una clase de tráfico de PIN o un tamaño de PIN.

- En algunas implementaciones, el método incluye además: recibir, de la estación base, un contenedor de políticas de UE que incluye al menos uno de: un identificador de PIN, una
10 indicación de si informar el establecimiento de PIN a la estación base, o uno o más conjuntos de las reglas de la política de selección de ruta del UE (URSP, en inglés) para el tráfico de PIN.

En algunas implementaciones, cada uno del uno o más conjuntos se asocia con un conjunto respectivo de atributos de PIN.

- 15 En algunas implementaciones, el método incluye además: transmitir una solicitud de establecimiento de PIN a la estación base; recibir un mensaje de aceptación de establecimiento de PIN de la estación base; y completar de manera responsiva el establecimiento de PIN.

- En algunas implementaciones, la solicitud de establecimiento de PIN incluye al menos uno de un identificador de PIN o un identificador del UE, y el mensaje de aceptación de
20 establecimiento de PIN incluye al menos una de una duración de PIN o una restricción de ubicación.

- En algunas implementaciones, el método incluye además: recibir el tráfico de la aplicación del al menos otro dispositivo; determinar las reglas de la política de selección de ruta del UE (URSP) para el tráfico de la aplicación; y basado en las reglas de la URSP, iniciar el
25 establecimiento de una sesión de unidad de datos de protocolo (PDU, en inglés) para enrutar el tráfico de la aplicación.

En algunas implementaciones, el método incluye además: transmitir una solicitud de suministro de política del EU a la estación base; y recibir un comando de políticas de UE de la estación base, donde el comando de políticas de UE incluye al menos uno de: un identificador de PIN, una indicación de si informar el establecimiento de PIN a la estación base, o las reglas de la política de selección de ruta del UE (URSP) para el tráfico de PIN.

En algunas implementaciones, la transmisión de la solicitud de suministro de políticas de UE se realiza en respuesta a la determinación de que el UE no tiene políticas válidas para la PIN.

En algunas implementaciones, el método incluye además: transmitir, a través de la señalización de la capa de aplicación, uno o más atributos de PIN a una función de aplicación (AF, en inglés) de PIN; y recibir, de la estación base, un contenedor de políticas de UE que incluye al menos uno de: un identificador de PIN, una indicación de si informar el establecimiento de PIN a la estación base, o las reglas de la política de selección de ruta del UE (URSP) para el tráfico de PIN, donde las reglas de la URSP se basan en uno o más atributos de PIN. Las reglas de la URSP pueden incluir además criterios de validación de selección de ruta, que restringen el establecimiento de la sesión de PDU relacionada con la PIN a una ubicación y tiempo específicos.

En algunas implementaciones, el método incluye además: recibir el tráfico de la aplicación del al menos otro dispositivo; determinar las reglas de la política de selección de ruta del UE (URSP) para el tráfico de PIN; y basado en las reglas de la URSP, determinar el establecimiento de una nueva sesión de unidad de datos de protocolo (PDU) con configuraciones de PIN especificadas, las configuraciones de PIN especificadas que incluyen un nombre de red de datos (DNN, en inglés) dedicado y una información de asistente de selección de segmentos de red de servicio (S-NSSAI, en inglés); y transmitir una solicitud de establecimiento de sesión de PDU a la estación base.

De acuerdo con otro aspecto de la presente descripción, un método incluye: recibir, de un equipo de usuario (UE), una solicitud de registro que incluye una capacidad del UE para servir como puerta de enlace para una red personal de Internet de las cosas (PIN); determinar, basado en los datos de suscripción para el UE, que se autoriza al UE a servir como la puerta de enlace para la PIN; y transmitir, al UE, un mensaje de aceptación de registro que incluye una autorización de puerta de enlace de PIN.

Otras versiones incluyen sistemas, aparatos y programas informáticos correspondientes para realizar las acciones de los métodos definidos por instrucciones codificadas en dispositivos de almacenamiento legibles por computadora. Estas y otras versiones pueden incluir opcionalmente una o más de las siguientes características.

En algunas implementaciones, el método incluye además: determinar, basado en los datos de suscripción para el UE, una o más políticas de PIN para la PIN; y transmitir la una o más políticas de PIN al UE.

En algunas implementaciones, la una o más políticas de PIN incluyen al menos uno de: un identificador de PIN, una indicación de si informar el establecimiento de PIN a la estación base, o las reglas de la política de selección de ruta del UE (URSP) para el tráfico de PIN. En algunas implementaciones, la una o más políticas de PIN se reciben de una función de aplicación (AF) de PIN.

En algunas implementaciones, la una o más políticas de PIN son políticas de PIN predeterminadas.

En algunas implementaciones, el método incluye además: recibir una solicitud de establecimiento de PIN del UE, la solicitud de establecimiento de PIN que incluye al menos uno de: un identificador de PIN, un identificador de UE, o uno o más atributos de PIN; suministrar, basado en los datos de suscripción para el UE, una o más restricciones para la PIN; y comunicar un mensaje de aceptación de establecimiento de PIN al UE, el mensaje de aceptación de establecimiento de PIN que incluye una o más restricciones para la PIN.

En algunas implementaciones, el método incluye además: en respuesta a la recepción de la solicitud de establecimiento de PIN, activar una notificación de exposición de eventos a una función de aplicación (AF) de PIN, la notificación de exposición de eventos que incluye uno o más atributos de PIN; recibir una o más políticas de PIN de la AF de PIN; determinar, basado en la una o más políticas, una actualización de políticas de PIN para proporcionar al UE; y comunicar la actualización de políticas de PIN al UE.

En algunas implementaciones, el método incluye además: recibir, del UE, una solicitud para establecer una nueva sesión de unidad de datos de protocolo (PDU), la solicitud que incluye un nombre de red de datos (DNN) dedicado y una información de asistente de selección de segmentos de red de servicio (S-NSSAI); determinar, basado en una o más políticas de gestión de sesión (SM), que se permite al UE establecer la nueva sesión de PDU en un tiempo actual y una ubicación de UE actual; y comunicarse con una función de aplicación (AF) de PIN para realizar la autenticación y autorización secundarias de la solicitud para establecer la nueva sesión de PDU, donde la AF de PIN sirve como una entidad de autenticación, autorización, contabilidad (AAA, en inglés) de red de datos (DN, en inglés).

Los detalles de una o más modalidades de estos sistemas y métodos se establecen en las figuras adjuntas y la descripción a continuación. Otras características, objetos, y ventajas de estos sistemas y métodos resultarán evidentes a partir de la descripción y las figuras, y de las reivindicaciones.

BREVE DESCRIPCIÓN DE LAS FIGURAS

La Figura 1 ilustra un sistema ilustrativo que incluye redes personales de Internet de las cosas (IoT) (PIN) de acuerdo con algunas modalidades.

La Figura 2 ilustra una interfaz común para elementos de PIN de acuerdo con algunas modalidades.

La Figura 3 ilustra un diagrama en bloque que muestra el manejo de políticas de PIN de acuerdo con algunas modalidades.

La Figura 4A ilustra un flujo de llamada para el suministro de parámetros de PIN de acuerdo con algunas modalidades.

- 5 La Figura 4B ilustra un flujo de llamada para la notificación de parámetros de PIN de acuerdo con algunas modalidades.

La Figura 5A ilustra un flujo de llamada para el establecimiento de PIN con suministro previo de políticas de PIN de acuerdo con algunas modalidades.

- 10 La Figura 5B ilustra un flujo de llamada alternativo para el establecimiento de PIN con suministro previo de políticas de PIN de acuerdo con algunas modalidades.

La Figura 6 ilustra un flujo de llamada para la autorización basada en el plano de usuario para el establecimiento de PIN de acuerdo con algunas modalidades.

La Figura 7 ilustra un flujo de llamada para el establecimiento de PIN con actualizaciones dinámicas de políticas de acuerdo con algunas modalidades.

- 15 La Figura 8A ilustra un flujo de llamada para la creación iniciada por el UE de una nueva PIN de acuerdo con algunas modalidades.

La Figura 8B ilustra un flujo de llamada para la creación iniciada por el UE de una nueva PIN con la participación de una AF de PIN de acuerdo con algunas modalidades.

- 20 La Figura 9A ilustra un diagrama de flujo de un método ilustrativo de acuerdo con algunas modalidades.

La Figura 9B ilustra un diagrama de flujo de otro método ilustrativo de acuerdo con algunas modalidades.

La Figura 10 ilustra un equipo de usuario (UE), de acuerdo con algunas modalidades.

La Figura 11 ilustra un nodo de acceso, de acuerdo con algunas modalidades.

- 25 La Figura 12 ilustra una arquitectura de un sistema que incluye una red central (CN), de acuerdo con algunas modalidades.

DESCRIPCIÓN DETALLADA

Una de las características que está desarrollando el Proyecto de Asociación de Tercera Generación (3GPP) es una red personal de Internet de las cosas (IoT) (PIN). Una PIN puede operarse en cooperación con una red móvil terrestre pública doméstica (PLMN, en inglés) proporcionada por un operador de red móvil (MNO). Como un ejemplo, una PIN puede operarse en cooperación con un sistema 3GPP de 5.^a generación (5GS, en inglés). Una PIN puede incluir, entre otras cosas, equipos de usuario (UE) celular y dispositivos de IoT. Entre muchos ejemplos, los dispositivos de IoT incluyen dispositivos de comunicación de tipo máquina (MTC, en inglés), dispositivos de vehículo a todo (V2X) y dispositivos usables. Un dispositivo que forma parte de una PIN se denomina “elemento” de esa PIN. Uno de los elementos de una PIN tiene una capacidad de gestión activa (PEMC) y el mismo u otro elemento tiene una capacidad de puerta de enlace activa (PEGC). Un PEMC es responsable de gestionar una PIN, y un PEGC es responsable de enrutar las comunicaciones entre la PIN y los sistemas externos (p. ej., un 5GS o un servidor en la nube). Generalmente, un elemento de PIN puede ser cualquier dispositivo inalámbrico y no se limita a ser un dispositivo inalámbrico basado en 3GPP. Sin embargo, un elemento de PIN que sirve como un PEMC, un PEGC o ambos es un dispositivo inalámbrico basado en 3GPP (o un dispositivo compatible con 3GPP) para que el elemento pueda comunicarse con una red asociada con la PIN.

Algunas de las características de PIN suministradas por 3GPP incluyen que un elemento de PIN se puede autenticar sin usar credenciales de 3GPP, un elemento de PIN puede ser miembro de diferentes PIN, un elemento de PIN no necesita ser un suscriptor del mismo MNO que el (los) elemento(s) de PIN que sirve(n) como PEGC/PEMC, y la comunicación entre los elementos podría ser usando métodos que no son 3GPP (p. ej., Bluetooth®, Wi-Fi, WLAN, etc.) o métodos 3GPP (p. ej., ProSe PC5 enlace directo). Sin embargo, las PIN siguen en desarrollo y actualmente existen muchos desafíos no abordados que enfrenta la adopción

de PIN. Un desafío es la falta de interoperatividad entre los elementos de una PIN. Este desafío se debe a que diferentes tipos de dispositivos usan diferentes protocolos de conectividad. Otro problema es cómo mejorar las capacidades del equipo de usuario (UE) con capacidades de gestión y puerta de enlace (p. ej., PEGC, PEMC). Otro desafío es la

5 privacidad del usuario. Específicamente, no hay técnicas existentes para entregar sólo la información necesaria a la red asociada mientras se preserva la privacidad del usuario.

En la presente descripción se describen soluciones que abordan muchos de los desafíos abiertos que enfrenta la adopción de PIN. Entre otras cosas, esta descripción describe atributos de PIN, aspectos arquitectónicos de PIN, configuraciones para la autorización de

10 PEGC/PEMC, configuraciones para la operación de PIN en conexión con una red asociada, identificadores para el establecimiento de PIN y parámetros de políticas, procedimientos para la notificación y suministro de parámetros, establecimiento de PIN con políticas suministradas previamente o con políticas dinámicas, y establecimiento de PIN dinámica iniciado por el UE. Esta descripción también describe métodos y sistemas para

15 implementar las soluciones descritas.

La Figura 1 ilustra un sistema ilustrativo 130 que incluye redes personales de Internet de las cosas (IoT) (PIN) 100 y 102 de acuerdo con algunas modalidades. Las PIN 100, 102 se operan en cooperación con un sistema de comunicación inalámbrica asociado. Para fines de conveniencia y sin limitación alguna, el sistema 130 se describe en el contexto de los

20 estándares de comunicación de nueva radio (NR, en inglés) de quinta generación (5G) como se define en las especificaciones técnicas del 3GPP. Por ejemplo, el sistema de comunicación inalámbrica asociado con las PIN 100, 102 puede ser un 5GS. Sin embargo, otros tipos de sistemas de comunicación son posibles, incluidos los sistemas heredados de 3GPP, p. ej., sistemas de evolución a largo plazo (LTE), y los futuros sistemas de 3GPP (p. ej., sistemas de

25 sexta generación [6G]), protocolos IEEE 802.16 (p. ej., WMAN, WiMAX, etc.), o lo similar. Si bien los aspectos pueden describirse en la presente descripción usando terminología asociada

comúnmente con 5G NR, los aspectos de la presente descripción pueden aplicarse a otros sistemas, tales como 3G, 4G y/o sistemas después de 5G (p. ej., 6G).

En algunas modalidades, las PIN 100, 102 pueden ser redes domésticas inteligentes, redes de dispositivos usables u otros tipos de redes. Como se muestra en la Figura 1, la

5 PIN 100 (también etiquetada como “PIN1”) y la PIN 102 (también etiquetada como “PIN2”) incluyen una pluralidad de elementos. En algunas modalidades, un dispositivo puede ser un elemento de más de una PIN. En el ejemplo de la Figura 1, el UE 106 es un elemento de ambas PIN 100, 102. El PIN 100 también incluye el elemento 104 (también etiquetado como “E1”), y la PIN 102 también incluye el elemento 108 (también etiquetado como “E2”)

10 y el elemento 110 (también etiquetado como “E3”). En el sistema 130, el UE 106 es un dispositivo basado en 3GPP y los elementos 104, 108, 110 pueden ser dispositivos basados en 3GPP o dispositivos no basados en 3GPP. Además, el UE 106 se configura como PEGC y PEMC de las PIN 100, 102. Como tal, el UE 106 sirve como una puerta de enlace entre las PIN 100, 102 y los sistemas externos. En la Figura 1, el UE 106 sirve
15 como una puerta de enlace entre las PIN 100, 102 y el 5GS asociado por medio de la red de acceso de radio (RAN, en inglés) 114. El UE 106 también puede servir como una puerta de enlace a otros sistemas externos, como la nube 112. Como se muestra en la Figura 1, el UE 106 usa los enlaces 116, 118, 120, 122, 124 para comunicarse con E1, E2, E3, nube 112 y RAN 114, respectivamente. Cabe señalar que los enlaces 116, 118 y
20 120 se representan usando dos líneas para representar las conexiones a la RAN y la nube, pero cada uno de los enlaces puede ser una única conexión con el UE 106.

En un ejemplo, las PIN 100, 102 pueden crearse por un usuario, p. ej., usando un UE de PEMC.

En otro ejemplo, las PIN 100, 102 se pueden crear mediante una función de aplicación (AF) dedicada a las PIN (también denominada “AF de PIN”). En aun otro ejemplo, las PIN 100, 102

25 pueden crearse por el 5GS asociado con las PIN. Como se describe con mayor detalle más abajo, el 5GS también puede gestionar el suministro de políticas de PIN, la autenticación de elementos y la incorporación de elementos para las PIN 100, 102.

En algunas modalidades, se asigna a cada una de las PIN 100, 102 uno o más atributos, p. ej., después de la creación de la PIN. Un atributo de PIN es indicativo de una característica operativa de la PIN correspondiente. Los atributos, que pueden proporcionarse al 5GS, permiten al MNO prestar un mejor servicio a la PIN, por ejemplo, al personalizar el servicio proporcionado a la PIN basado en los atributos de PIN. Como un ejemplo, el MNO puede definir y asignar políticas para una PIN basadas en los atributos de ese PIN. Más específicamente, el MNO puede permitir que solo ciertos tipos de las PIN opere en cooperación con el 5GS, el MNO puede proporcionar diferentes servicios a diferentes tipos de PIN, y/o el MNO puede asignar diferentes prioridades a diferentes tipos de PIN.

En algunas modalidades, los atributos de PIN incluyen una clase de PIN (p. ej., una indicación del tipo de dispositivos en la PIN), un alcance de tráfico de PIN (p. ej., una indicación de la ubicación del tráfico de PIN), una clase de tráfico de PIN (p. ej., prioridad del tráfico de PIN) y un tamaño de PIN (p. ej., una indicación de un tamaño de PIN). Las categorías dentro de la clase de PIN incluyen una PIN privada (p. ej., red doméstica), una PIN pública (p. ej., centro comercial) y una PIN de área corporal personal (p. ej., reloj inteligente, gafas inteligentes). Las categorías dentro del alcance de tráfico de PIN incluyen: (i) local (p. ej., el flujo de tráfico se mantiene dentro de la PIN), (ii) parcialmente local (p. ej., algunos elementos envían tráfico al 5GS asociado), y (iii) en la nube (p. ej., los elementos de PIN se comunican con un servidor en la nube). Las categorías dentro de la clase de tráfico de PIN incluyen tráfico de alta prioridad y tráfico de baja prioridad. El tamaño de PIN es un tamaño de PIN que se compartirá con la red. El tamaño de PIN puede definirse de diferentes maneras, p. ej., número de elementos (un número exacto o un rango), una carga agregada de PIN, ciclo de trabajo de los elementos de PIN, entre otros ejemplos. Otros atributos de PIN y categorías dentro de los atributos de PIN son posibles y se contemplan en la presente descripción.

En algunas modalidades, los elementos de una PIN se configuran con una capa de PIN que sirve como una interfaz común para intercambiar información entre los elementos de PIN.

Específicamente, la capa de PIN puede usarse para intercambiar información entre las PIN que pueden tener diferentes protocolos de comunicación. Por lo tanto, la capa de PIN permite a los dispositivos comunicarse sin problemas dentro de la PIN. Por ejemplo, la salida de la capa de PIN puede proporcionarse al (a los) dispositivo(s) PEGC/PEMC, que, como se indicó anteriormente, son compatibles con 3GPP y pueden comunicarse con el 5GS asociado. Como otro ejemplo, la capa de PIN también podría usarse como una capa de comunicación entre los elementos de PIN y la red 3GPP.

La Figura 2 ilustra una interfaz común para elementos de PIN de acuerdo con algunas modalidades. En un ejemplo, el E1, E2, E3 y UE son similares al E1, E2, E3 y UE 106, respectivamente, de la Figura 1. Como se muestra en la Figura 2, cada elemento de PIN incluye una capa de PIN respectiva además del protocolo del elemento de PIN respectivo. Por ejemplo, además del Protocolo 1, E1 también incluye una capa de PIN respectiva. Las capas de PIN respectivas interactúan con las capas de protocolo respectivas y entre sí.

En algunas modalidades, el 5GS asociado con una PIN realiza procesos de autorización y suministro de políticas para las PIN. Como se describe con mayor detalle más abajo, los procesos de autorización y suministro de políticas pueden iniciarse por un UE que está sirviendo como PEGC. Los procesos de autorización y suministro de políticas pueden usar los datos de suscripción de ese UE. En algunos ejemplos, los datos de suscripción de un UE incluyen (i) una autorización para actuar como un PEGC y/o un PEMC, y/o (ii) la información que indica si se permite al UE solicitar dinámicamente la creación de una nueva PIN. La autorización para actuar como PEGC y/o PEMC puede ser una autorización abierta (p. ej., un UE tiene autorización para actuar como PEGC y/o PEMC para cualquier PIN) o puede ser una autorización restringida (p. ej., un UE tiene autorización para actuar como PEGC y/o PEMC para PIN específicas).

En algunas modalidades, las políticas para una PIN se proporcionan por una AF. En ejemplos donde el sistema asociado es 5GS, la AF puede ser una AF de 5G existente que se ha modificado para incluir capacidades de gestión de PIN dedicadas. Tal AF se denomina "AF de

PIN” en la presente descripción. Alternativamente, las políticas pueden configurarse localmente por el MNO del 5GS. Tal configuración es aplicable en escenarios donde la PIN es propiedad/está gestionada por el MNO o cuando las políticas de PIN son estáticas y, por lo tanto, no se necesita una AF de PIN de terceros. Cabe señalar que una AF puede controlarse por un MNO o puede controlarse por un tercero. En el primer escenario, la AF es parte de la red central 5G. En el segundo escenario, la AF se denomina AF de terceros.

En algunas modalidades, una función de control de políticas (PCF, en inglés) del 5GS también se configura con políticas predeterminadas para configuraciones de PIN. Como se describe más abajo, las políticas predeterminadas se pueden usar para las PIN creadas dinámicamente por un UE. A una PIN también se le puede asignar un identificador. Dentro de los ejemplos, un identificador de PIN puede suministrarse previamente (p. ej., una configuración de AF de PIN o una configuración de MNO local) o crearse dinámicamente (p. ej., xyz@pin.[AMF identifier].mnc013.mcc234.3gpp). En algunos ejemplos, el MNO puede tener una configuración centralizada para garantizar identificadores de PIN únicos. Alternativamente, un identificador de PIN podría incluir un identificador de función de gestión de acceso y movilidad (AMF) como parte del identificador de PIN, lo que asegura identificadores de PIN únicos.

La Figura 3 ilustra un diagrama en bloque 300 que ilustra el manejo de políticas de PIN de acuerdo con algunas modalidades. Específicamente, la Figura 3 ilustra cómo las políticas de PIN se manejan por la gestión unificada de datos (UDM) 302, la PCF 304 y la AF de PIN 306. La UDM 302 y la PCF 304 son parte de la red central del 5GS. Como se muestra en el bloque 308, la UDM 302 almacena datos de suscripción del UE, que pueden incluir la autorización de un UE para actuar como un PEGC y/o un PEMC. En escenarios donde se restringe la autorización, los datos de suscripción del UE pueden incluir identificadores de las PIN en las que el UE tiene autorización para actuar como PEGC y/o PEMC. Adicionalmente y/o alternativamente, los datos de suscripción del UE pueden incluir una indicación de si se permite

al UE solicitar dinámicamente la creación de una nueva PIN (p. ej., sin autorización previa por parte del MNO).

Como se muestra en el bloque 310, las políticas específicas de una PIN se crean por la AF de PIN 306 y almacenadas en la PCF 304. En algunos ejemplos, las políticas de PIN incluyen
5 selección de ruta, información sobre el tamaño de PIN (p. ej. un número máximo de dispositivos), restricciones de tiempo y/o ubicación, y/o una indicación de si el 5GS tiene que participar en la creación de la PIN. Como se muestra en el bloque 312, la PCF 304 se puede configurar adicionalmente y/o alternativamente con una configuración de PIN predeterminada para asignarse a una PIN creada dinámicamente. Como se describe con
10 mayor detalle más abajo, una PIN creada dinámicamente no tiene ninguna solicitud de AF de PIN. Como se muestra en el bloque 314, los identificadores PIN se pueden suministrar previamente o crear dinámicamente.

En algunas modalidades, una AF de PIN es responsable de suministrar los parámetros de PIN al 5GS. Los atributos de PIN, p. ej., el tamaño de red, el rendimiento (p. ej., expresado como
15 velocidad de bits máxima agregada) y la capacidad, se pueden usar como parámetros de PIN. Además, la AF de PIN puede suscribirse al 5GS para recibir notificaciones relacionadas con las PIN. Por ejemplo, la AF de PIN puede suscribirse a notificaciones relacionadas con las redes PIN que cumplen criterios específicos.

La Figura 4A ilustra un flujo de llamada 400 para el suministro de parámetros de PIN de acuerdo con algunas modalidades. El flujo de llamada 400 es una versión modificada del suministro de parámetros descrito en la TS del 3GPP 23.502, Sección 4.15.6.2. Como se muestra en la Figura 4A, la instancia 402 del repositorio de datos de usuario (UDR, en inglés), la UDM 404, la función de exposición de red (NEF, en inglés) 406 y la AF de PIN 408 participan en el suministro de parámetros. Como se muestra en el bloque 410, la AF de PIN 408 invoca
20 Nnef_ParameterProvision_Create para un nuevo evento de creación de PIN. La AF de PIN 408 incluye parámetros de políticas de PIN en el mensaje invocado que se envía a la NEF 406. Como se muestra en el bloque 412, la NEF 406 envía a la UDM 404 una solicitud

Nudm_ParameterProvision_Create. Como se muestra en el bloque 414, el UDR 402 y la UDM 404 se actualizan con los parámetros de políticas proporcionados por la AF de PIN 408. Una vez que la UDM 404 completa el procedimiento con el UDR 402, se envía una respuesta de suministro de parámetros a la AF de PIN 408, tal vez por la NEF 406. Como se muestra en el

5 bloque 416, la UDM 404 puede generar notificaciones indicativas de los parámetros de políticas de PIN a una PCF del 5GS.

La Figura 4B ilustra un flujo de llamada 420 para la notificación de parámetros de PIN de acuerdo con algunas modalidades. El flujo de llamada 420 es una versión modificada de la notificación de parámetros descrita en la TS del 3GPP 23.502, Sección 4.15.3.2.3. Como

10 se muestra en la Figura 4B, la AMF 422, UDM 404, NEF 406 y AF de PIN 408 participan en el flujo de llamada 420. Como se muestra en el bloque 424, la AF de PIN 408 invoca Nnef_EventExposure_Subscribe para un nuevo evento de creación de PIN. La AF de PIN 408 incluye características de PIN en el mensaje invocado que se envía a la NEF 406. Como se muestra en el bloque 426, la NEF 406 y la UDM 404 crean una suscripción de

15 exposición de eventos para la AF de PIN 408 basada en las características de PIN proporcionadas. Como se muestra en el bloque 428, la UDM 404 usa un servicio de suscripción de exposición de eventos de AMF 422 para el evento de creación de PIN.

En algunas modalidades, los UE compatibles con 3GPP y el 5GS se configuran para realizar flujos de trabajo para establecer y configurar redes PIN. Los flujos de trabajo pueden incluir

20 uno o más de: (i) un primer flujo de trabajo para el establecimiento de PIN con suministro previo de políticas de PIN, (ii) un segundo (o alternativo) flujo de trabajo para el establecimiento de PIN con suministro previo de políticas de PIN, (iii) un flujo de trabajo para la autorización del plano de usuario para el establecimiento de PIN, (iv) un flujo de trabajo para el establecimiento de PIN con actualizaciones dinámicas de políticas, (v) un flujo de trabajo para la creación

25 iniciada por el UE de una nueva PIN, (vi) un flujo de trabajo para la creación iniciada por el UE de una nueva PIN con la participación de una AF de PIN.

Cada uno de estos flujos de trabajo se describe con mayor detalle en relación con las figuras 5A-8B. La Figura 5A ilustra un flujo de llamada 500 para el establecimiento de PIN con suministro previo de políticas de PIN. La Figura 5B ilustra un flujo de llamada alternativo 550 para el establecimiento de PIN con suministro previo de políticas de PIN. La Figura 6 ilustra un flujo de llamada 600 para la autorización basada en el plano de usuario para el establecimiento de PIN. La Figura 7 ilustra un flujo de llamada 700 para el establecimiento de PIN con actualizaciones dinámicas de políticas. La Figura 8A ilustra un flujo de llamada 800 para la creación iniciada por el UE de una nueva PIN. La Figura 8B ilustra un flujo de llamada 850 para la creación iniciada por el UE de una nueva PIN con la participación de una AF de PIN. En los ejemplos de estas figuras, la PIN que se establece incluye un dispositivo basado en 3GPP (UE-1) y otros dos dispositivos (E1, E2), que pueden ser dispositivos basados en 3GPP o no 3GPP. El UE-1 sirve como el PEGC y PEMC de PIN que se está estableciendo. Además, el 5GS incluye NG-RAN 502, AMF 504, función de gestión de sesión (SMF, en inglés) 506, UDM 508, PCF 510 y NEF 512. El 5GS se comunica con la AF de PIN 514, que puede ser una AF confiable o no confiable. Cabe señalar que otras disposiciones ilustrativas son posibles. También, cabe señalar que los flujos de llamada descritos se pueden aplicar a otros sistemas de comunicación inalámbrica.

Con respecto a la Figura 5A, el flujo de llamada 500 es para el establecimiento de PIN usando políticas suministradas previamente de la AF de PIN 514. Como se muestra en el bloque 516, la AF de PIN 514 usa un proceso de suministro de parámetros (a través de NEF 512) para actualizar la red central con políticas de PIN. Como un ejemplo, la AF de PIN 514 puede usar el flujo de llamada 400 del suministro de políticas de PIN descrito en la Figura 4A. El flujo de llamada 500 se basa en un procedimiento de registro descrito en la TS del 3GPP 23.502, Sección 4.2.2.2, y un procedimiento de establecimiento de sesión de PDU descrito en la TS del 3GPP 23.502, Sección 4.3.2.2.

En la Etapa 1, el UE-1 se registra en la red central del 5GS asociado. En esta etapa, el UE-1 genera una solicitud de registro que se envía, a través de NG-RAN 502, a AMF 504. La

solicitud de registro incluye un contenedor de políticas de UE que incluye las capacidades relacionadas con la PIN del UE-1 (p. ej., capacidad PEGC y/o capacidad PEMC). En este ejemplo, el contenedor de políticas de UE incluye una indicación de las capacidades de PEGC y PEMC. En la Etapa 2, la AMF 504 comprueba los datos de suscripción del UE-1, p. ej., al comunicarse con SMF 506 y/o UDM 508, y determinar si se permite al UE-1 actuar como PEGC/PEMC. En la Etapa 3, y en respuesta a la determinación de que se permite al UE-1 actuar como PEGC/PEMC, la AMF 504 envía al UE-1 un mensaje de aceptación de registro. Entre otras cosas, el mensaje de aceptación de registro incluye autorizaciones de UE relacionadas con la PIN. Por ejemplo, el mensaje de aceptación de registro puede incluir una autorización de puerta de enlace de PIN, una autorización de PIN dinámica (p. ej., si se permite al UE-1 crear dinámicamente nuevas PIN), entre otra información.

En la Etapa 4, el contenedor de políticas de UE se pasa a la PCF 510. En la Etapa 4a, la PCF 510 consulta a la UDM 508 para recuperar una o más políticas de PIN aplicables a la suscripción del UE-1. Las políticas aplicables al UE pueden incluir uno o más conjuntos de atributos de PIN y las políticas correspondientes, incluida la URSP. En la Etapa 4b, la PCF

510 envía una solicitud a la AMF 504 para proporcionar una o más políticas de PIN al UE-1. La solicitud puede enviarse en un mensaje "Namf_Communication_N1N2MessageTransfer". En algunos ejemplos, las políticas de PIN incluyen un identificador de PIN, una indicación de si debe informarse a la red central de la creación de PIN y/o las reglas de la política de selección de ruta de UE (URSP) para el tráfico de PIN. Las restricciones de ubicación y tiempo para el tráfico de PIN pueden expresarse como criterios de validación de selección de ruta en la regla de la URSP correspondiente a la PIN. Entonces, el UE que actúa como PEGC toma en consideración las restricciones al iniciar el establecimiento de la sesión de PDU para el tráfico de PIN. Cabe señalar que la red central (p. ej., la AMF) puede requerir que se le informe de la creación de PIN si se aplica cierta restricción de tiempo/ubicación a las operaciones de

PIN. Adicionalmente y/o alternativamente, las políticas de PIN pueden incluir políticas que se aplican a cualquier PIN creada en la red aplicable.

En la Etapa 5, la AMF 504 pasa el contenedor de políticas de UE al UE-1. En la Etapa 6, el UE-1, E1 y E2 inician el establecimiento de PIN. En los ejemplos donde debe informarse a

5 la red central de la creación de la PIN, se realizan las Etapas 7-9. En la Etapa 7, el UE-1 informa a la red central de la creación de la PIN, p. ej., al enviar una solicitud de establecimiento de PIN a la AMF 504. La solicitud puede incluir un identificador de PIN y/o identificadores del UE (o de los UE) que operan como PEGC y PEMC. En este ejemplo, la solicitud incluye un identificador de PIN y un identificador de UE-1 (como PEGC/PEMC). En

10 la Etapa 8, la AMF 504 comprueba si existen restricciones locales aplicables a la PIN, p. ej., al comprobar la suscripción del UE-1, las políticas de PIN aplicables y/o las configuraciones de AMF. Como un ejemplo, basado en las restricciones identificadas, la AMF 504 puede limitar la operación de la PIN a un cierto tiempo o a una cierta ubicación (p. ej., para un sistema doméstico inteligente instalado y mantenido por el MNO para una ubicación

15 doméstica de un suscriptor). Las restricciones pueden ser en toda el área de seguimiento (TA, en inglés) o específicas de la celda. En la Etapa 9, la AMF 504 confirma al UE-1 el establecimiento de PIN e incluye información adicional sobre las restricciones (si las hubiera). Por ejemplo, la información adicional puede incluir una duración de PIN y/o una restricción de ubicación.

20 En la Etapa 10, se completa el establecimiento de PIN. En esta etapa, el UE-1 también selecciona las políticas de PIN aplicables basado en las características de PIN que se establece. En la Etapa 11, el tráfico de la aplicación que se origina en uno de los elementos de PIN se dirige a un servidor en la nube (no se muestra en la Figura 5A). Específicamente, el tráfico de la aplicación se envía al UE-1, ya que sirve como la puerta de enlace para la PIN. En

25 la Etapa 12, el UE-1 evalúa las reglas de la URSP para establecer una sesión de PDU (p. ej., si aún no se ha establecido una sesión de PDU). En este ejemplo, las reglas de la URSP activan el establecimiento de una sesión de PDU. En la Etapa 13, se establece la sesión de

PDU (o se modifica si ya se ha establecido una sesión de PDU). En la Etapa 14, la SMF 506 obtiene las políticas de gestión de sesión (SM) aplicables a la PIN y enruta el tráfico de PIN en consecuencia.

La Figura 5B ilustra un flujo de llamada alternativo 550 para el establecimiento de PIN usando políticas suministradas previamente. El flujo de llamada 550 puede usarse en escenarios de suministro de políticas iniciado por el UE. En estos escenarios, el UE-1 es responsable de iniciar el suministro de políticas. En consecuencia, el UE-1 se comunica directamente con la PCF 510 para solicitar políticas de PIN.

En las Etapas 1-3, el UE-1 realiza el registro de UE al comunicarse con la AMF 504. Estas etapas son similares a las Etapas 1-3 del flujo de llamada 500. Como se muestra en el bloque 552, el UE-1, en respuesta a la recepción del mensaje de aceptación de registro de AMF 504, determina que no tiene políticas válidas para servir como la puerta de enlace de PIN y activa el suministro de políticas (es decir, suministro de políticas iniciado por el UE). Específicamente, en la Etapa 4, el UE-1 envía una solicitud de suministro de políticas de UE a la PCF 510. La solicitud puede incluir una capacidad de puerta de enlace de PIN. En la Etapa 5, la PCF 510 consulta a la UDM 508 para recuperar las políticas de PIN aplicables a la suscripción del UE-1. En la Etapa 6, la PCF 510 envía al UE-1 un comando de gestión de políticas de UE. El comando puede incluir un identificador de PIN, una indicación de si debe informarse a la red central de la creación de PIN y las reglas de la URSP para el tráfico de PIN. Como se muestra en estas etapas, el UE-1 es responsable de iniciar el suministro de políticas. Esto contrasta con el suministro de políticas que inicia la red central, como se realiza en el flujo de llamada 500. Las Etapas 7-15 son similares a las Etapas 6-14 de la Figura 5A, respectivamente.

La Figura 6 ilustra un flujo de llamada 600 para la autorización basada en el plano de usuario para el establecimiento de PIN. En algunos ejemplos, el flujo de llamada 600 se usa en escenarios donde la PIN se configura para establecer una sesión de PDU separada para el tráfico de PIN.

En el flujo de llamada 600, la Etapa 1 de registro de UE y la Etapa 2 de actualizaciones de políticas de UE son similares a las Etapas 1-5 del flujo de llamada 500 o las Etapas 1-6 del flujo de llamada 550 (p. ej., dependiendo de si el suministro de políticas es iniciado por la red o el UE). En la Etapa 3, la PIN se establece localmente entre el UE-1, E1 y E2. En la Etapa 4, el tráfico de la aplicación de los elementos de PIN activa el UE-1, que sirve como PEGC. En la Etapa 5, el UE-1 evalúa las reglas de la URSP para la PIN. En este ejemplo, las reglas de la URSP indican que la PIN se configura para establecer una sesión de PDU separada (p. ej., separada de la sesión de PDU para el tráfico de UE). Basado en la evaluación de las reglas de la URSP, el UE-1 procede a establecer una nueva sesión de PDU con las configuraciones de PIN especificadas por las reglas de la URSP. Las configuraciones de PIN pueden incluir un nombre de red de datos (DNN) dedicado y una información de asistente de selección de segmentos de red de servicio (S-NSSAI).

En la Etapa 6, el UE-1 envía una solicitud de establecimiento de sesión de PDU a la SMF 506. En la Etapa 7, basado en las políticas de SM, la SMF 506 evalúa si se le permite establecer la nueva sesión de PDU en el tiempo actual y desde la ubicación del UE-1. Si la SMF 506 determina que se le permite establecer la nueva sesión de PDU, la SMF 506 contacta a la AF de PIN 514, que actúa como una entidad de autenticación, autorización, contabilidad (AAA) de red de datos (DN), para realizar la autenticación y autorización secundarias. En la Etapa 8, la AF de PIN 514 procede con la autenticación y autorización secundarias (p. ej., como se describe en la TS del 3GPP 23.501, Sección 5.6.6).

La Figura 7 ilustra el flujo de llamada 700 para el establecimiento de PIN con actualizaciones dinámicas de políticas. En algunos ejemplos, el flujo de llamada 700 se utiliza para establecer una PIN usando políticas dinámicas proporcionadas por el UE-1.

En las Etapas 1-3, el UE-1 realiza el registro de UE al comunicarse con la AMF 504. Estas etapas son similares a las Etapas 1-3 del flujo de llamada 500 de la Figura 5A. En la Etapa 4, se establece la PIN. En la Etapa 5, el UE-1 intercambia información de PIN con la AF de PIN 514, tal vez usando la señalización de la capa de aplicación. La información de PIN puede

incluir las políticas de PIN del UE-1. Las políticas de PIN del UE-1 pueden, por ejemplo, especificarse por uno o más usuarios de PIN. En este caso, el UE-1 informa a la AF de PIN sobre las características (o atributos) de PIN como parte del intercambio de información de PIN de la capa de aplicación. En la Etapa 6, la AF de PIN 514 proporciona las políticas de PIN a la

5 PCF 510. En las Etapas 7-9, se informa a la red central del establecimiento de PIN. Específicamente, en la etapa 7, el UE-1 envía una solicitud de establecimiento de PIN a la AMF 504. La solicitud puede incluir un identificador de PIN e identificadores del uno o más UE que sirve(n) como PEMC y PEGC. En la Etapa 8, la AMF 504 establece las restricciones de PIN basadas en uno o más de (i) los datos de suscripción del UE-1, (ii) las políticas de PIN

10 aplicables y (iii) las configuraciones de la AMF. En la Etapa 9, la AMF 504 envía al UE-1 un mensaje de aceptación de establecimiento de PIN que incluye una duración de PIN y/o restricciones de ubicación (p. ej., restricciones en toda el TA o específicas de la celda). En algunos ejemplos, la AMF 504 puede proporcionar al UE-1 políticas de PIN predeterminadas que se usarán hasta que el UE-1 pueda actualizarse con políticas específicas de PIN.

15 En la Etapa 10, la PCF 510 envía una actualización de políticas a la AMF 504 (p. ej., basada en las actualizaciones de políticas recibidas en la Etapa 6), tal vez en un mensaje `Namf_communication_N1N2_MessageTransfer`. Las políticas de PIN pueden incluir un identificador de PIN y/o las reglas de la URSP para el tráfico de PIN. A su vez, la AMF 504 envía la actualización de políticas al UE-1, tal vez en un mensaje de contenedor de políticas

20 de UE. En la Etapa 12, se confirma el establecimiento de PIN. Las Etapas 13-16 implican el tráfico de la aplicación de PIN que activa el establecimiento de una sesión de PDU (p. ej., como se describe en el flujo de llamada 500).

La Figura 8A ilustra el flujo de llamada 800 para el establecimiento de PIN iniciado por el UE. En las Etapas 1-3, el UE-1 realiza el registro de UE al comunicarse con la AMF 504. Estas

25 etapas son similares a las Etapas 1-3 del flujo de llamada 500 de la Figura 5A. En la Etapa 4, se realiza el descubrimiento de los elementos de PIN y el establecimiento de PIN. El descubrimiento y el establecimiento de PIN son interacciones de la capa de aplicación. En la

Etapa 5, el UE-1 informa a la red central de PIN recién establecida, tal vez por medio de una solicitud de establecimiento de PIN enviada a la AMF 504. La solicitud de establecimiento de PIN puede incluir un identificador de la nueva PIN y/o características de PIN (p. ej., tipo de PIN, número de elementos de PIN y/o clase de tráfico). Adicionalmente y/o alternativamente, el UE-1 proporciona atributos de PIN como parte de la solicitud de establecimiento de PIN. En algunos ejemplos, el UE-1 puede autoasignar un identificador de PIN (de acuerdo con los parámetros de MNO configurados). En la Etapa 6, la AMF 504 proporciona restricciones de PIN, p. ej., basadas en (i) la suscripción del UE-1, (ii) las políticas de PIN aplicables y (iii) las configuraciones de AMF. Además, la AMF 504 asigna un identificador de PIN a la PIN (p. ej., confirma un identificador de PIN proporcionado por el UE o asigna un nuevo identificador de PIN). En la Etapa 7, la AMF 504 genera un evento para la creación de PIN y activa una exposición de eventos a través de la NEF 512 a la AF de PIN 514. La comunicación de exposición de eventos puede incluir un nuevo evento de creación de PIN con un ID único. En la Etapa 7a, la AF de PIN 514 decide las políticas de PIN para la PIN creada. En la Etapa 7b, la AF de PIN 514 suministra políticas de PIN específicas para la PIN. En algunas modalidades, se informa a la AF de PIN 514 de la creación de la PIN a través de la señalización de la capa de aplicación del UE-1. En estas modalidades, se omite la Etapa 7.

En la Etapa 8, se confirma el establecimiento de PIN al UE-1. Específicamente, la AMF 504 puede enviar al UE-1 un mensaje de aceptación de establecimiento de PIN que incluye una asignación de identificador de PIN, una duración de PIN y/o una restricción de ubicación (si la hubiera). En la Etapa 9, la PCF 510 determina las políticas de PIN que se proporcionarán al UE-1 basado en las políticas suministradas de la AF de PIN 514. En la Etapa 10, las políticas de PIN determinadas se proporcionan a la AMF 504. En la Etapa 10a, la AMF envía las políticas suministradas al UE-1 en un contenedor de políticas de UE. En la Etapa 11, se completa el establecimiento de PIN. Las Etapas 12-15 implican el tráfico de la aplicación de PIN que activa el establecimiento de una sesión de PDU (p. ej., como se describe en el flujo de llamada 500).

La Figura 8B ilustra el flujo de llamada 850 para un establecimiento de PIN iniciado por el UE con la participación de la AF de PIN 514. Generalmente, el flujo de llamada 850 es similar al flujo de llamada 800 excepto en las Etapas 6-7. En la Etapa 6 del flujo de llamada 850, la AMF 504 genera un evento para la creación de PIN y activa una exposición de eventos a través de la NEF 512 a la AF de PIN 514. Y en la Etapa 7, la AF de PIN 514 asigna identificadores de PIN (confirma o vuelve a asignar un identificador de PIN si el UE-1 ya había proporcionado uno). La AF de PIN 514 también proporciona restricciones de PIN. El flujo de llamada 850 permite a la AF de PIN 514 controlar directamente la autorización del establecimiento de instancias de PIN y establecer las condiciones adecuadas para las operaciones.

La Figura 9A ilustra un diagrama de flujo de un método ilustrativo 900 de acuerdo con algunas implementaciones. Para mayor claridad de la presentación, la descripción que sigue describe generalmente el método 900 en el contexto de las otras figuras de esta descripción. Por ejemplo, el método 900 puede realizarse por el UE 106 de la Figura 1. Se entenderá que el método 900 puede realizarse, por ejemplo, por cualquier sistema, entorno, software, hardware, o una combinación de sistemas, entornos, software y hardware adecuados, según corresponda. En algunas implementaciones, diversas etapas del método 900 pueden ejecutarse en paralelo, en combinación, en bucles, o en cualquier orden.

En la Etapa 902, el método 900 implica generar una solicitud de registro que comprende una capacidad del UE para servir como una puerta de enlace para una red personal de Internet de las cosas (PIN).

En la Etapa 904, el método 900 implica enviar la solicitud de registro a una estación base que sirve al UE.

En la Etapa 906, el método 900 recibe, de la estación base, un mensaje de aceptación de registro que comprende una autorización de puerta de enlace de PIN.

En la Etapa 908, el método 900 implica iniciar el establecimiento de PIN con al menos otro dispositivo, en donde el UE sirve como la puerta de enlace de PIN a la estación base.

En algunas implementaciones, la solicitud de registro incluye además uno o más atributos de PIN.

- 5 En algunas implementaciones, uno o más atributos de PIN incluyen al menos uno de: una clase de PIN, un alcance de tráfico de PIN que proporciona una ubicación de tráfico de PIN, una clase de tráfico de PIN o un tamaño de PIN.

- En algunas implementaciones, el método incluye además: recibir, de la estación base, un contenedor de políticas de UE que incluye al menos uno de: un identificador de PIN, una
10 indicación de si informar el establecimiento de PIN a la estación base, o uno o más conjuntos de las reglas de la política de selección de ruta del UE (URSP) para el tráfico de PIN.

En algunas implementaciones, cada uno del uno o más conjuntos se asocia con un conjunto respectivo de atributos de PIN.

- 15 En algunas implementaciones, el método incluye además: transmitir una solicitud de establecimiento de PIN a la estación base; recibir un mensaje de aceptación de establecimiento de PIN de la estación base; y completar de manera responsiva el establecimiento de PIN.

- En algunas implementaciones, la solicitud de establecimiento de PIN incluye al menos uno de un identificador de PIN o un identificador del UE, y el mensaje de aceptación de
20 establecimiento de PIN incluye al menos una de una duración de PIN o una restricción de ubicación.

- En algunas implementaciones, el método incluye además: recibir el tráfico de la aplicación del al menos otro dispositivo; determinar las reglas de la política de selección de ruta del UE (URSP) para el tráfico de la aplicación; y basado en las reglas de la URSP,
25 iniciar el establecimiento de una sesión de unidad de datos de protocolo (PDU) para enrutar el tráfico de la aplicación.

En algunas implementaciones, el método incluye además: transmitir una solicitud de suministro de política del EU a la estación base; y recibir un comando de políticas de UE de la estación base, donde el comando de políticas de UE incluye al menos uno de: un identificador de PIN, una indicación de si informar el establecimiento de PIN a la estación base, o las reglas de la política de selección de ruta del UE (URSP) para el tráfico de PIN.

En algunas implementaciones, la transmisión de la solicitud de suministro de políticas de UE se realiza en respuesta a la determinación de que el UE no tiene políticas válidas para la PIN.

En algunas implementaciones, el método incluye además: transmitir, a través de la señalización de la capa de aplicación, uno o más atributos de PIN a una función de aplicación (AF) de PIN; y recibir, de la estación base, un contenedor de políticas de UE que incluye al menos uno de: un identificador de PIN, una indicación de si informar el establecimiento de PIN a la estación base, o las reglas de la política de selección de ruta del UE (URSP) para el tráfico de PIN, donde las reglas de la URSP se basan en uno o más atributos de PIN.

En algunas implementaciones, el método incluye además: recibir el tráfico de la aplicación del al menos otro dispositivo; determinar las reglas de la política de selección de ruta del UE (URSP) para el tráfico de PIN; y basado en las reglas de la URSP, determinar el establecimiento de una nueva sesión de unidad de datos de protocolo (PDU) con configuraciones de PIN especificadas, las configuraciones de PIN especificadas que incluyen un nombre de red de datos (DNN) dedicado y una información de asistente de selección de segmentos de red de servicio (S-NSSAI); y transmitir una solicitud de establecimiento de sesión de PDU a la estación base.

La Figura 9B ilustra un diagrama de flujo de un método ilustrativo 920 de acuerdo con algunas implementaciones. Para mayor claridad de la presentación, la descripción que sigue describe generalmente el método 920 en el contexto de las otras figuras de esta

descripción. Por ejemplo, el método 920 puede realizarse por la CN 1220 de la Figura 12. Se entenderá que el método 920 puede realizarse, por ejemplo, por cualquier sistema, entorno, software, hardware, o una combinación de sistemas, entornos, software y hardware adecuados, según corresponda. En algunas implementaciones, diversas etapas del método 920 pueden ejecutarse en paralelo, en combinación, en bucles, o en cualquier orden.

En 922, el método 920 implica recibir, de un equipo de usuario (UE), una solicitud de registro que comprende una capacidad del UE para servir como una puerta de enlace para una red personal de Internet de las cosas (PIN).

10 En 924, el método 900 implica determinar, basado en los datos de suscripción para el UE, que se autoriza al UE a servir como la puerta de enlace para la PIN.

En 926, el método 900 implica transmitir, al UE, un mensaje de aceptación de registro que comprende una autorización de puerta de enlace de PIN.

15 En algunas implementaciones, el método incluye además: determinar, basado en los datos de suscripción para el UE, una o más políticas de PIN para la PIN; y transmitir la una o más políticas de PIN al UE.

En algunas implementaciones, la una o más políticas de PIN incluyen al menos uno de: un identificador de PIN, una indicación de si informar el establecimiento de PIN a la estación base, o las reglas de la política de selección de ruta del UE (URSP) para el tráfico de PIN.

20 En algunas implementaciones, la una o más políticas de PIN se reciben de una función de aplicación (AF) de PIN.

En algunas implementaciones, la una o más políticas de PIN son políticas de PIN predeterminadas.

25 En algunas implementaciones, el método incluye además: recibir una solicitud de establecimiento de PIN del UE, la solicitud de establecimiento de PIN que incluye al menos uno de: un identificador de PIN, un identificador de UE, o uno o más atributos de PIN; suministrar, basado en los datos de suscripción para el UE, una o más restricciones

para la PIN; y comunicar un mensaje de aceptación de establecimiento de PIN al UE, el mensaje de aceptación de establecimiento de PIN que incluye una o más restricciones para la PIN.

En algunas implementaciones, el método incluye además: en respuesta a la recepción de la solicitud de establecimiento de PIN, activar una notificación de exposición de eventos a una función de aplicación (AF) de PIN, la notificación de exposición de eventos que incluye uno o más atributos de PIN; recibir una o más políticas de PIN de la AF de PIN; determinar, basado en la una o más políticas, una actualización de políticas de PIN para proporcionar al UE; y comunicar la actualización de políticas de PIN al UE.

En algunas implementaciones, el método incluye además: recibir, del UE, una solicitud para establecer una nueva sesión de unidad de datos de protocolo (PDU), la solicitud que incluye un nombre de red de datos (DNN) dedicado y una información de asistente de selección de segmentos de red de servicio (S-NSSAI); determinar, basado en una o más políticas de gestión de sesión (SM), que se permite al UE establecer la nueva sesión de PDU en un tiempo actual y una ubicación de UE actual; y comunicarse con una función de aplicación (AF) de PIN para realizar la autenticación y autorización secundarias de la solicitud para establecer la nueva sesión de PDU, donde la AF de PIN sirve como una entidad de autenticación, autorización, contabilidad (AAA) de red de datos (DN).

La Figura 10 ilustra un UE 1000 de acuerdo con algunas modalidades. El UE 1000 puede ser similar a y sustancialmente intercambiable con el UE 106 de la Figura 1.

El UE 1000 puede ser cualquier dispositivo informático móvil o no móvil, tal como, por ejemplo, teléfonos móviles, computadoras, tabletas, sensores inalámbricos industriales (por ejemplo, micrófonos, sensores de dióxido de carbono, sensores de presión, sensores de humedad, termómetros, sensores de movimiento, acelerómetros, escáneres láser, sensores de nivel de fluidos, sensores de inventario, medidores de corriente/voltaje eléctrico, actuadores, etc.), dispositivos de videovigilancia/monitoreo (por ejemplo, cámaras o cámaras de video, etc.), dispositivos usables (por ejemplo, un reloj inteligente), o dispositivo de Internet de las Cosas.

El UE 1000 puede incluir procesadores 1002, sistema de circuitos de interfaz de RF 1004, memoria/almacenamiento 1006, interfaz de usuario 1008, sensores 1010, sistema de circuitos del controlador 1012, circuito integrado de gestión de energía (PMIC, en inglés) 1014, estructura de antena 1016 y batería 1018. Los componentes del UE 1000 pueden implementarse como circuitos integrados (IC, en inglés), porciones de estos, dispositivos electrónicos discretos, u otros módulos, lógica, hardware, software, firmware, o una combinación de estos. El diagrama en bloque de la Figura 10 pretende mostrar una vista de alto nivel de algunos de los componentes del UE 1000. Sin embargo, algunos de los componentes mostrados pueden omitirse, pueden estar presentes componentes adicionales, y se puede producir diferente disposición de los componentes en otras implementaciones.

Los componentes del UE 1000 pueden acoplarse con otros diversos componentes a través de una o más interconexiones 1020, que pueden representar cualquier tipo de interfaz, entrada/salida, bus (local, sistema o expansión), línea de transmisión, traza, conexión óptica, etc. que permite que diversos componentes de circuito (en chips o conjuntos de chips comunes o diferentes) interactúen entre sí.

Los procesadores 1002 pueden incluir sistema de circuitos de procesador tales como, por ejemplo, sistema de circuitos del procesador de banda base (BB) 1022A, sistema de circuitos de la unidad de procesador central (CPU, en inglés) 1022B, y sistema de circuitos de la unidad de procesador de gráficos (GPU, en inglés) 1022C. Los procesadores 1002 pueden incluir cualquier tipo de sistema de circuitos o sistema de circuitos de procesador que ejecuta o de cualquier otra manera opera instrucciones ejecutables por computadora, tales como código de programa, módulos de software, o procesos funcionales de memoria/almacenamiento 1006 para hacer que el UE 1000 realice operaciones como se describe en la presente descripción.

En algunas modalidades, el sistema de circuitos de procesador de banda base 1022A puede acceder a una pila de protocolos de comunicación 1024 en la memoria/almacenamiento 1006 para comunicarse a través de una red compatible con 3GPP. Generalmente, el sistema de circuitos de procesador de banda base 1022A puede

acceder a la pila de protocolos de comunicación para: realizar funciones de plano de usuario en una capa PHY, capa MAC, capa RLC, capa PDCP, capa SDAP, y capa PDU; y realizar funciones del plano de control en una capa PHY, capa MAC, capa RLC, capa PDCP, capa RRC, y una capa de estrato sin acceso. En algunas modalidades, las

5 operaciones de la capa PHY se pueden realizar adicionalmente/alternativamente por los componentes del sistema de circuitos de interfaz de RF 1004. El sistema de circuitos de procesador de banda base 1022A puede generar o procesar señales de banda base o formas de onda que llevan información en redes compatibles con 3GPP. En algunas modalidades, las formas de onda para NR pueden basarse en la OFDM con prefijo cíclico

10 “CP-OFDM” (en inglés) en el enlace ascendente o descendente, y la OFDM con dispersión de transformación discreta de Fourier “DFT-S-OFDM” (en inglés) en el enlace ascendente. La memoria/almacenamiento 1006 puede incluir uno o más medios no transitorios legibles por computadora, que incluyen instrucciones (por ejemplo, la pila de protocolos de comunicación 1024) que pueden ejecutarse por uno o más de los procesadores 1002 para hacer que el UE

15 1000 realice diversas operaciones descritas en la presente descripción. La memoria/almacenamiento 1006 incluye cualquier tipo de memoria volátil o no volátil que puede distribuirse en todo el UE 1000. En algunas modalidades, parte de la memoria/almacenamiento 1006 puede ubicarse en los procesadores 1002 en sí (por ejemplo, caché L1 y L2), mientras que otra memoria/almacenamiento 1006 es externa a los procesadores 1002 pero accesible a

20 estos a través de una interfaz de memoria. La memoria/almacenamiento 1006 puede incluir cualquier memoria volátil o no volátil adecuada tal como, pero sin limitarse a, memoria de acceso aleatorio dinámico (DRAM, en inglés), memoria de acceso aleatorio estático (SRAM, en inglés), memoria de solo lectura programable borrrable (EPROM, en inglés), memoria de solo lectura programable borrrable eléctricamente (EEPROM, en inglés), memoria Flash,

25 memoria de estado sólido, o cualquier otro tipo de tecnología de dispositivos de memoria. El sistema de circuitos de interfaz de RF 1004 puede incluir sistemas de circuitos de transceptor y módulo frontal de frecuencia de radio (RFEM, en inglés) que permite que el UE 1000 se

comunique con otros dispositivos a través de una red de acceso de radio. El sistema de circuitos de interfaz de RF 1004 puede incluir diversos elementos dispuestos en trayectos de transmisión o recepción. Estos elementos pueden incluir, por ejemplo, conmutadores, mezcladores, amplificadores, filtros, sistemas de circuitos de sintetizador, sistemas de circuitos de control, etc.

En el trayecto de recepción, el RFEM puede recibir una señal radiada de una interfaz aérea a través de la estructura de antena 1016 y proceder a filtrar y amplificar (con un amplificador de bajo ruido) la señal. La señal puede proporcionarse a un receptor del transmisor que convierte la señal de RF en una señal de banda base que se proporciona al procesador de banda base de los procesadores 1002.

En el trayecto de transmisión, el transmisor del transmisor aumenta la frecuencia de la señal de banda base recibida del procesador de banda base y proporciona la señal de RF al RFEM. El RFEM puede amplificar la señal de RF a través de un amplificador de potencia antes de que la señal se irradie a través de la interfaz aérea mediante la antena 1016.

En diversas modalidades, se puede configurar el sistema de circuitos de interfaz de RF 1004 para transmitir/recibir señales de una manera compatible con las tecnologías de acceso de NR.

La antena 1016 puede incluir elementos de antena para convertir señales eléctricas en ondas de radio para desplazarse por el aire y convertir las ondas de radio recibidas en señales eléctricas. Los elementos de antena pueden disponerse en uno o más paneles de antena. La antena 1016 pueden tener paneles de antena que son omnidireccionales, direccionales, o una combinación de estos para permitir la formación de haces y las comunicaciones de múltiples entradas y múltiples salidas. La antena 1016 puede incluir antenas de microtira, antenas impresas fabricadas sobre la superficie de una o más placas de circuito impreso, antenas de parche, antenas de matriz de fase, etc. La antena 1016 puede tener uno o más paneles diseñados para bandas de frecuencia específica que incluyen bandas en FR1 o FR2.

La interfaz de usuario 1008 incluye diversos dispositivos de entrada/salida (I/O) diseñados para permitir la interacción del usuario con el UE 1000. La interfaz de usuario 1008 incluye el sistema de circuitos de dispositivo de entrada y el sistema de circuitos de dispositivo de salida. El sistema de circuitos del dispositivo de entrada incluye cualquier medio físico o virtual para

5 aceptar una entrada que incluye, entre otros, uno o más botones físicos o virtuales (p. ej., un botón de reinicio), un teclado físico, teclado numérico, mouse, almohadilla táctil, pantalla táctil, micrófonos, escáner, auricular y/o lo similar. El sistema de circuitos de dispositivo de salida incluye cualquier medio físico o virtual para mostrar información o transmitir información, tales como lecturas del sensor, posición(es) del accionador u otra información similar. El sistema de

10 circuitos del dispositivo de salida puede incluir cualquier número o combinaciones de pantallas de audio o visuales, que incluyen, inter alia, una o más salidas/indicadores visuales simples (por ejemplo, indicadores de estado binario tales como los diodos emisores de luz “LED” (en inglés) y las salidas visuales de multicaracteres), o salidas más complejas tales como dispositivos de visualización o pantallas táctiles (por ejemplo, pantallas de cristal líquido “LCD”

15 (en inglés), pantallas LED, pantallas de puntos cuánticos, proyectores, etc.), con la salida de caracteres, gráficos, objetos multimedia, y lo similar que se generan o producen a partir de la operación del EU 1000.

Los sensores 1010 incluyen dispositivos, módulos, o subsistemas cuyo propósito es detectar eventos o cambios en su entorno y enviar la información (datos de sensor) sobre los eventos

20 detectados a algún otro dispositivo, módulo, subsistema, etc. Ejemplos de tales sensores incluyen, inter alia, unidades de medición de inercia que comprenden acelerómetros, giroscopios, o magnetómetros; sistemas microelectromecánicos o sistemas nanoelectromecánicos que comprenden acelerómetros de 3 ejes, giroscopios de 3 ejes y/o magnetómetros; sensores de nivel; sensores de flujo; sensores de temperatura (por ejemplo,

25 termistores); sensores de presión; sensores de presión barométrica; gravímetros; altímetros; dispositivos de captura de imágenes (por ejemplo, cámaras o aperturas de lente); sensores de detección de luz y alcance; sensores de proximidad (por ejemplo, detector de radiación

infrarroja y lo similar); sensores de profundidad; sensores de luz ambiental; transceptores ultrasónicos; micrófonos u otros dispositivos de captura de audio; etc.

El sistema de circuitos del controlador 1012 puede incluir elementos de software y hardware que operan para controlar dispositivos particulares que se integran en el UE 1000, acoplados

5 al UE 1000, o acoplados comunicativamente de cualquier otra manera con el UE 1000. El sistema de circuitos del controlador 1012 puede incluir controladores individuales que permiten que otros componentes interactúen con o controlen diversos dispositivos de entrada/salida (E/S) que puedan estar presentes dentro de, o conectados a, el UE 1000. Por ejemplo, el sistema de circuitos del controlador 1012 puede incluir un controlador de pantalla para controlar
10 y permitir el acceso a un dispositivo de visualización, un controlador de pantalla táctil para controlar y permitir el acceso a una interfaz de pantalla táctil, controladores de sensor para obtener lecturas de sensores 1010 y controlar y permitir el acceso a los sensores 1010, controladores para obtener posiciones de actuador de componentes electromecánicos o controlar y permitir el acceso a los componentes electromecánicos, un controlador de cámara
15 para controlar y permitir el acceso a un dispositivo de captura de imágenes integrado, controladores de audio para controlar y permitir el acceso a uno o más dispositivos de audio. El PMIC 1014 puede gestionar la energía proporcionada a diversos componentes del UE 1000. En particular, con respecto a los procesadores 1002, el PMIC 1014 puede controlar la selección de la fuente de energía, el escalado de voltaje, la carga de la batería o la
20 conversión de CC a CC.

En algunas modalidades, el PMIC 1014 puede controlar, o de cualquier otra manera ser parte de, diversos mecanismos de ahorro de energía del UE 1000 que incluye DRX como se describe en la presente descripción. Una batería 1018 puede alimentar el UE 1000, aunque en algunos ejemplos el UE 1000 puede montarse desplegado en una ubicación fija, y puede tener una
25 fuente de alimentación acoplada a una red eléctrica. La batería 1018 puede ser una batería de iones de litio, una batería de metal-aire, tal como una batería de zinc-aire, una batería de aluminio-aire, una batería de litio-aire y lo similar. En algunas implementaciones, tales como

en aplicaciones basadas en vehículos, la batería 1018 puede ser una batería típica automotriz de plomo-ácido.

La Figura 11 ilustra un nodo de acceso 1100 (p. ej., una estación base o gNB) de acuerdo con algunas modalidades. El nodo de acceso 1100 puede incluir procesadores 1102, sistemas de circuitos de interfaz de RF 1104, sistemas de circuitos de interfaz de red central (CN, en inglés) 1106, sistemas de circuitos de memoria/almacenamiento 1108 y una estructura de antena 1110.

Los componentes del nodo de acceso 1100 pueden acoplarse con otros componentes diversos a través de una o más interconexiones 1112. Los procesadores 1102, el sistema de circuitos de interfaz de RF 1104, el sistema de circuitos de memoria/almacenamiento 1108 (que incluye la pila de protocolos de comunicación 1114), la estructura de antena 1110 y las interconexiones 1112 pueden ser similares a los elementos con nombres similares mostrados y descritos con respecto a la Figura 10. Por ejemplo, los procesadores 1102 pueden incluir sistemas de circuitos de procesador tales como, por ejemplo, sistemas de circuitos del procesador de banda base (BB) 1116A, sistemas de circuitos de la unidad de procesador central (CPU) 1116B, y sistemas de circuitos de la unidad de procesador de gráficos (GPU) 1116C.

El sistema de circuitos de la interfaz de CN 1106 puede proporcionar conectividad a una red central, por ejemplo, una red central de quinta generación (5GC, en inglés) que usa un protocolo de interfaz de red compatible con 5GC, tal como protocolos Ethernet del portador, o algún otro protocolo adecuado. La conectividad de red puede proporcionarse hacia/desde el nodo de acceso 1100 mediante una red de redireccionamiento inalámbrica o de fibra óptica. El sistema de circuitos de la interfaz de CN 1106 puede incluir uno o más procesadores dedicados y/o las FPGA para comunicarse usando uno o más de los protocolos mencionados anteriormente. En algunas implementaciones, el sistema de circuitos de la interfaz de CN 1106 puede incluir múltiples controladores para proporcionar conectividad a otras redes usando los mismos o diferentes protocolos.

Como se usa en la presente descripción, los términos “nodo de acceso”, “punto de acceso” o lo similar pueden describir un equipo que proporciona la función de banda base de radio para datos y/o conectividad de voz entre una red y uno o más usuarios. Estos nodos de acceso pueden denominarse BS, gNB, nodos RAN, eNB, Nodob, RSU, TRxP o TRP, etc., y pueden comprender estaciones de suelo (p. ej., puntos de acceso terrestre) o estaciones satélite que proporcionan cobertura dentro de un área geográfica (p. ej., una celda). Como se usa en la presente descripción, el término “nodo NG RAN” o lo similar puede referirse a un nodo de acceso 1100 que opera en un sistema NR o 5G (por ejemplo, un gNB), y el término “nodo E-UTRAN” o lo similar puede referirse a un nodo de acceso 1100 que opera en un sistema LTE o 4G (p. ej., un eNB). De acuerdo con diversas implementaciones, el nodo de acceso 1100 pueden implementarse como uno o más de un dispositivo físico dedicado, tal como una estación base de macroceldas, y/o una estación base de baja potencia (LP, en inglés) para proporcionar femtoceldas, picoceldas u otras celdas similares que tienen áreas de cobertura más pequeñas, capacidad de usuario más pequeña, o ancho de banda más alta en comparación con las macroceldas. En algunas modalidades, todos o partes de los nodos de acceso 1100 pueden implementarse como una o más entidades de software que se ejecutan en computadoras de servidores como parte de una red virtual, que puede denominarse CRAN y/o un conjunto de unidades de banda base virtual (vBBUP, en inglés). En estas modalidades, la CRAN o vBBUP puede implementar una división de función de RAN, tal como una división de PDCP, en donde las capas de RRC y PDCP se operan por la CRAN/vBBUP y otras entidades del protocolo L2 se operan por el nodo de acceso 1100; una división MAC/PHY en donde las capas de RRC, PDCP, RLC y MAC se operan por la CRAN/vBBUP y la capa PHY se opera por el nodo de acceso 1100; o una división “inferior de PHY” en donde las capas de RRC, PDCP, RLC, MAC y porciones superiores de la capa PHY se operan por la CRAN/vBBUP y las porciones inferiores de la capa PHY se operan por el nodo de acceso 1100.

En escenarios V2X, el nodo de acceso 1100 puede ser o actuar como RSU. El término “unidad lateral de carretera” o “RSU” puede referirse a cualquier entidad de infraestructura de transporte usada para comunicaciones V2X. Una RSU puede implementarse en o por un nodo RAN adecuado o un UE estacionario (o relativamente estacionario), donde una RSU implementada en o por un UE puede denominarse como una “RSU tipo UE”, una RSU implementada en o por un eNB puede denominarse una “RSU tipo eNB”, una RSU implementada en o por un gNB puede denominarse “RSU tipo gNB”, y lo similar.

La Figura 12 ilustra una arquitectura de un sistema 1200 que incluye una red central (CN) 1220 de acuerdo con diversas modalidades. Se muestra que el sistema 1200 incluye un UE 1201, que puede ser el mismo o similar al UE 1000 descrito anteriormente; una (R)AN 1210, que puede ser la misma o similar a la RAN 114 descrita anteriormente; y una DN 1203, que puede ser, por ejemplo, servicios de operador, acceso a Internet o servicios de terceros; y una 5GC 1220. La 5GC 1220 puede incluir una AUSF 1222; una AMF 1221; una SMF 1224; una NEF 1223; una PCF 1226; una NRF 1225; una UDM 1227; una AF 1228; una UPF 1202; y una NSSF 1229. En algunas modalidades, la AMF 1221 puede ser la misma o similar a la AMF 422 de la Figura 4B y/o la AMF 504 de las Figuras 5A-8B. La AF 1228 puede ser la misma o similar a la AF de PIN 306 de la Figura 3, la AF de PIN 408 de las Figuras 4A-4B y/o la AF de PIN 514 de las Figuras 5A-8B. La UDM 1227 puede ser la misma o similar a la UDM 404 de las Figuras 4A-4B y/o la UDM 508 de las Figuras 5A-8B. La NEF 1223 puede ser la misma o similar a la NEF 406 de las Figuras 4A-4B y/o la NEF 512 de las Figuras 8A-8B. La SMF 1224 puede ser la misma o similar a la SMF 506 de las Figuras 5A-8B, y la PCF 1226 puede ser la misma o similar a la PCF 510 de las Figuras 5A-8B. La RAN 1210 puede ser la misma o similar a la NG-RAN 502 de las Figuras 5A-8B.

La UPF 1202 puede actuar como un punto de anclaje para la movilidad intra-RAT e inter-RAT, un punto de sesión de PDU externo de interconexión a la DN 1203, y un punto de ramificación para soportar una sesión de PDU de multiconexión. La UPF 1202 también

puede realizar el enrutamiento y reenvío de paquetes, realizar la inspección de paquetes, hacer cumplir la parte del plano de usuario de las reglas de política, interceptar paquetes legalmente (recopilación de UP), realizar informes de uso de tráfico, realizar el manejo de QoS para un plano de usuario (p. ej., filtrado de paquetes, puerta de enlace, cumplimiento de velocidad de UL/DL), realizar la verificación de tráfico de enlace ascendente (p. ej., mapeo de flujo de SDF a QoS), marcado de paquetes a nivel de transporte en el enlace ascendente y descendente, y realizar el almacenamiento en búfer de los paquetes de enlace descendente y la activación de notificaciones de datos de enlace descendente. La UPF 1202 puede incluir un clasificador de enlace ascendente para soportar flujos de tráfico de enrutamiento a una red de datos. La DN 1203 puede representar diversos servicios de operador de red, acceso a Internet, o servicios de terceros. La DN 1203 puede incluir, o ser similar al servidor de aplicaciones XQ30 descrito anteriormente. La UPF 1202 puede interactuar con la SMF 1224 a través de un punto de referencia N4 entre la SMF 1224 y la UPF 1202.

La AUSF 1222 puede almacenar datos para la autenticación del UE 1201 y manejar funcionalidades relacionadas con la autenticación. La AUSF 1222 puede facilitar un marco de autenticación común para diversos tipos de acceso. La AUSF 1222 puede comunicarse con la AMF 1221 a través de un punto de referencia N12 entre la AMF 1221 y la AUSF 1222; y puede comunicarse con la UDM 1227 a través de un punto de referencia N13 entre la UDM 1227 y la AUSF 1222. Además, la AUSF 1222 puede presentar una interfaz basada en el servicio Nausf.

La AMF 1221 puede ser responsable de la gestión del registro (p. ej., del registro del UE 1201, etc.), gestión de la conexión, gestión de la disponibilidad, gestión de la movilidad e interceptación legal de los eventos relacionados con la AMF, y autenticación y autorización del acceso. La AMF 1221 puede ser un punto de terminación para el punto de referencia N11 entre la AMF 1221 y la SMF 1224. La AMF 1221 puede proporcionar transporte para mensajes SM entre el UE 1201 y la SMF 1224, y actuar como un proxy transparente para enrutar los mensajes SM.

La AMF 1221 también puede proporcionar transporte para mensajes SMS entre el UE 1201 y una SMSF (no se muestra en la Figura 12). La AMF 1221 puede actuar como SEAF, lo que puede incluir la interacción con la AUSF 1222 y el UE 1201, la recepción de una clave intermedia que se estableció como resultado del proceso de autenticación del UE 1201. Donde se usa la autenticación basada en USIM, la AMF 1221 puede recuperar el material de seguridad de la AUSF 1222. La AMF 1221 también puede incluir una función de SCM, que recibe una clave del SEA que usa para derivar claves específicas de la red de acceso. Además, la AMF 1221 puede ser un punto de terminación de una interfaz RAN CP, que puede incluir o ser un punto de referencia de N2 entre la (R)AN 1210 y la AMF 1221; y la AMF 1221 puede ser un punto de terminación de señalización de NAS (N1), y realizar cifrado y protección de integridad de NAS.

La AMF 1221 también puede soportar la señalización de NAS con un UE 1201 sobre una interfaz N3 IWF. La N3IWF puede usarse para proporcionar acceso a entidades no confiables. La N3IWF puede ser un punto de terminación para la interfaz N2 entre la (R)AN 1210 y la AMF 1221 para el plano de control, y puede ser un punto de terminación para el punto de referencia N3 entre la (R)AN 1210 y la UPF 1202 para el plano de usuario. Como tal, la AMF 1221 puede manejar la señalización N2 a partir de la SMF 1224 y la AMF 1221 para sesiones de PDU y QoS, encapsular/desencapsular paquetes para la IPSec y el tunelado N3, marcar los paquetes del plano de usuario N3 en el enlace ascendente, y hacer cumplir la QoS correspondiente al marcado de paquetes N3 teniendo en cuenta los requisitos de QoS asociados con tal marcado recibido a través de N2. La N3IWF también puede transmitir la señalización de NAS del plano de control de enlace ascendente y enlace descendente entre el UE 1201 y la AMF 1221 por medio de un punto de referencia N1 entre el UE 1201 y la AMF 1221, y transmitir los paquetes de plano de usuario del enlace ascendente y enlace descendente entre el UE 1201 y la UPF 1202. La N3IWF también proporciona mecanismos para el establecimiento del túnel IPsec con el UE 1201. La AMF 1221 puede mostrar una interfaz basada en el servicio Namf, y puede ser

un punto de terminación para un punto de referencia N14 entre dos AMF 1221 y un punto de referencia N17 entre la AMF 1221 y un 5G-EIR (no se muestra en la Figura 12).

El UE 1201 puede necesitar registrarse en la AMF 1221 para recibir servicios de red. La RM se usa para registrar o anular el registro del UE 1201 en la red (p. ej., AMF 1221) y

5 establecer un contexto de UE en la red (p. ej., AMF 1221). El UE 1201 puede operar en un estado RM-REGISTERED o un estado RM-DEREGISTERED. En el estado RM DEREGISTERED, el UE 1201 no está registrado en la red, y el contexto de UE en la AMF 1221 no contiene información válida de ubicación o enrutamiento para el UE 1201, de manera que la AMF 1221 no puede acceder al UE 1201. En el estado RM REGISTERED,

10 el UE 1201 está registrado en la red, y el contexto de UE en la AMF 1221 puede contener una información válida de ubicación o enrutamiento para el UE 1201, de manera que el UE 1201 es accesible por la AMF 1221. En el estado RM-REGISTERED, el UE 1201 puede realizar procedimientos de actualización de registro de movilidad, realizar procedimientos de actualización de registro periódicos activados por la expiración del temporizador de
15 actualización periódica (p. ej., para notificar a la red que el UE 1201 todavía está activo), y realizar un procedimiento de actualización de registro para actualizar la información de capacidad del UE o para renegociar los parámetros de protocolo con la red, entre otros.

La AMF 1221 puede almacenar uno o más contextos de RM para el UE 1201, donde cada contexto de RM se asocia con un acceso específico a la red. El contexto de RM puede ser una

20 estructura de datos, un objeto de base de datos, etc., que indica o almacena, inter alia, un estado de registro por tipo de acceso y el temporizador de actualización periódica. La AMF 1221 también puede almacenar un contexto MM de 5GC que puede ser el mismo o similar al contexto (E)MM descrito anteriormente. En varias modalidades, la AMF 1221 puede almacenar un parámetro de restricción del modo B de CE del UE 1201 en un contexto MM o contexto RM
25 asociado. La AMF 1221 también puede derivar el valor, cuando sea necesario, del parámetro de configuración de uso del UE ya almacenado en el contexto de UE (y/o en el contexto MM/RM).

La CM puede usarse para establecer y liberar una conexión de señalización entre el UE 1201 y la AMF 1221 a través de la interfaz N1. La conexión de señalización se usa para permitir el intercambio de señalización de NAS entre el UE 1201 y la CN 1220, y comprende tanto la conexión de señalización entre el UE y la AN (p. ej., conexión RRC o conexión UE-N3IWF para el acceso no 3GPP) y la conexión N2 para el UE 1201 entre la AN (p. ej., RAN 1210) y la AMF 1221. El UE 1201 puede operar en uno de dos estados de CM, modo CM-IDLE o modo CM-CONNECTED. Cuando el UE 1201 está operando en el estado/modo CM-IDLE, el UE 1201 puede no tener conexión de señalización de NAS establecida con la AMF 1221 a través de la interfaz N1, y puede haber conexión de señalización (R)AN 1210 (p. ej., conexiones N2 y/o N3) para el UE 1201. Cuando el UE 1201 está operando en el estado/modo CM-CONNECTED, el UE 1201 puede tener una conexión de señalización de NAS establecida con la AMF 1221 a través de la interfaz N1, y puede haber una conexión de señalización (R)AN 1210 (p. ej., conexiones N2 y/o N3) para el UE 1201. El establecimiento de una conexión de N2 entre la (R)AN 1210 y la AMF 1221 puede hacer que el UE 1201 pase del modo CM-IDLE al modo CM-CONNECTED, y el UE 1201 puede pasar del modo CM-CONNECTED al modo CM-IDLE cuando se libera señalización N2 entre la (R)AN 1210 y la AMF 1221.

La SMF 1224 puede ser responsable de la SM (p. ej., establecimiento, modificación y liberación de sesiones, incluido el mantenimiento del túnel entre el nodo UPF y AN); asignación y manejo de dirección IP de UE (incluida la autorización opcional); selección y control de la función de UP; configurar el direccionamiento de tráfico a UPF para enrutar el tráfico al destino adecuado; terminación de interfaces hacia las funciones de control de políticas; controlar parte del cumplimiento de políticas y QoS; interceptación legal (para eventos de SM e interfaz al sistema LI); terminación de las partes SM de mensajes NAS; notificaciones de datos de enlace descendente; iniciar una información de SM específica, enviada a través de AMF sobre N2 a AN; y determinar el modo SSC de una sesión. La SM puede referirse a la gestión de una sesión de PDU, y una sesión de PDU o “sesión” puede referirse a un servicio de conectividad de PDU

que proporciona o permite el intercambio de las PDU entre un UE 1201 y una red de datos (DN) 1203 identificada por un nombre de red de datos (DNN). Las sesiones de PDU pueden establecerse a solicitud del UE 1201, modificarse a solicitud del UE 1201 y la 5GC 1220, y liberarse a solicitud del UE 1201 y la 5GC 1220 usando la señalización de SM de NAS intercambiada a través del punto de referencia N1 entre el UE 1201 y la SMF 1224. A solicitud de un servidor de aplicaciones, al 5GC 1220 puede activar una aplicación específica en el UE 1201. En respuesta a la recepción del mensaje de activación, el UE 1201 puede pasar el mensaje de activación (o partes/información relevante del mensaje de activación) a una o más aplicaciones identificadas en el UE 1201. La(s) solicitud(es) identificada(s) en el UE 1201 puede(n) establecer una sesión de PDU a un DNN específico. La SMF 1224 puede verificar si las solicitudes del UE 1201 cumplen con la información de suscripción de usuario asociada con el UE 1201. En este sentido, la SMF 1224 puede recuperar y/o solicitar recibir notificaciones de actualización sobre los datos de suscripción de nivel SMF 1224 de la UDM 1227.

La SMF 1224 puede incluir la siguiente funcionalidad de itinerancia: manejo del cumplimiento local para aplicar SLA QoS (VPLMN); cargar la recolección de datos y la interfaz de carga (VPLMN); interceptación legal (en VPLMN para eventos de SM e interfaz al sistema LI); y soporte para la interacción con DN externa para transporte de señalización para autorización/autenticación de sesión de PDU mediante DN externa. Puede incluirse un punto de referencia N16 entre dos SMF 1224 en el sistema 1200, que puede estar entre otra SMF 1224 en una red visitada y la SMF 1224 en la red doméstica en escenarios de itinerancia. Además, la SMF 1224 puede mostrar la interfaz basada en servicio de Nsmf.

La NEF 1223 puede proporcionar medios para exponer de manera segura los servicios y capacidades proporcionados por las funciones de red 3GPP para terceros, exposición/reexposición interna, funciones de aplicación (p. ej., AF 1228), sistemas informáticos de borde o niebla, etc. En tales modalidades, la NEF 1223 puede autenticar, autorizar y/o regular las AF. La NEF 1223 también puede trasladar la información intercambiada con la AF 1228 y la información intercambiada con funciones de red

interna. Por ejemplo, la NEF 1223 puede trasladarse entre un identificador de servicio de AF y una información interna de 5GC. La NEF 1223 también puede recibir información de otras funciones de red (NF) basadas en las capacidades expuestas de otras funciones de red. Esta información puede almacenarse en la NEF 1223 como datos estructurados, o en una NF de almacenamiento de datos usando interfaces estandarizadas. Después, la NEF 1223 puede volver a exponer la información almacenada a otras NF y AF, y/o usarla para otros fines tales como análisis. Además, la NEF 1223 puede mostrar una interfaz basada en el servicio de Nnef.

La NRF 1225 puede soportar funciones de descubrimiento de servicios, recibir solicitudes de descubrimiento de NF de instancias de NF, y proporcionar la información de las instancias de NF descubiertas a las instancias de NF. La NRF 1225 también mantiene información de instancias de NF disponibles y sus servicios soportados. Como se usa en la presente descripción, los términos “instanciar”, “instanciación” y lo similar pueden referirse a la creación de una instancia, y una “instancia” puede referirse a una ocurrencia concreta de un objeto, que puede ocurrir, por ejemplo, durante la ejecución del código de programa. Además, la NRF 1225 puede mostrar la interfaz basada en servicio de Nnrf.

La PCF 1226 puede proporcionar reglas de política a la(s) función(es) del plano de control para hacerlas cumplir, y también puede soportar el marco de política unificado para gobernar el comportamiento de la red. La PCF 1226 también puede implementar una FE para acceder a la información de suscripción relevante para las decisiones de política en un UDR de la UDM 1227. La PCF 1226 puede comunicarse con la AMF 1221 a través de un punto de referencia N15 entre la PCF 1226 y la AMF 1221, que puede incluir una PCF 1226 en una red visitada y la AMF 1221 en caso de escenarios de itinerancia. La PCF 1226 puede comunicarse con la AF 1228 a través de un punto de referencia N5 entre la PCF 1226 y la AF 1228; y con la SMF 1224 a través de un punto de referencia N7 entre la PCF 1226 y la SMF 1224. El sistema 1200 y/o la CN 1220 también puede incluir un punto de referencia N24 entre la PCF 1226 (en la red

doméstica) y una PCF 1226 en una red visitada. Además, la PCF 1226 puede mostrar una interfaz basada en el servicio de Npcf.

La UDM 1227 puede manejar la información relacionada con la suscripción para soportar el manejo de las sesiones de comunicación por parte de las entidades de red y puede

5 almacenar datos de suscripción del UE 1201. Por ejemplo, los datos de suscripción pueden comunicarse entre la UDM 1227 y la AMF 1221a través de un punto de referencia N8 entre la UDM 1227 y la AMF. La UDM 1227 puede incluir dos partes, una FE de aplicación y un UDR (la FE y el UDR no se muestran en la Figura 12). El UDR puede almacenar datos de suscripción y datos de políticas para la UDM 1227 y la PCF 1226, y/o datos estructurados

10 para exposición y datos de aplicación (que incluyen FDR para la detección de aplicación, información de solicitud de aplicación para múltiples UE 1201) para la NEF 1223. El UDR puede mostrar la interfaz basada en el servicio de Nudr para permitir el acceso de UDM 1227, PCF 1226, y NEF 1223 a un conjunto particular de datos almacenados, así como para leer, actualizar (p. ej., añadir, modificar), eliminar y suscribirse a la notificación de

15 cambios de datos relevantes en el UDR. La UDM puede incluir una UDM-FE, que se encarga del procesamiento de credenciales, gestión de ubicación, gestión de suscripción, etc. Varias terminales de entrada diferentes pueden servir al mismo usuario en diferentes transacciones. La UDM-FE tiene información de suscripción almacenada en el UDR y realiza el procesamiento de credenciales de autenticación, manejo de identificación del

20 usuario, autorización de acceso, gestión de registro/movilidad, y gestión de suscripción. El UDR puede interactuar con la SMF 1224 a través de un punto de referencia N10 entre la UDM 1227 y la SMF 1224. La UDM 1227 también puede soportar la gestión de SMS, en donde un SMS-FE implementa la lógica de aplicación similar a la descrita anteriormente. Además, la UDM 1227 puede mostrar la interfaz basada en el servicio de Nudm.

25 La AF 1228 puede proporcionar influencia en la aplicación en el enrutamiento de tráfico, proporcionar acceso a la NCE e interactuar con el marco de política para el control de políticas. La NCE puede ser un mecanismo que permite a la 5GC 1220 y la AF 1228

proporcionarse información entre sí a través de la NEF 1223, que puede usarse para implementaciones informáticas de borde. En tales implementaciones, el operador de red y los servicios de terceros pueden alojarse cerca del punto de acceso del UE 1201 para lograr una entrega de servicio eficiente a través de la reducción de latencia de extremo a extremo y la carga en la red de transporte. Para las implementaciones informáticas de borde, la 5GC puede seleccionar una UPF 1202 cerca del UE 1201 y ejecutar dirección del tráfico de la UPF 1202 a la DN 1203 a través de la interfaz N6. Esto puede basarse en los datos de suscripción del UE, la ubicación del UE y la información proporcionada por la AF 1228. De esta manera, la AF 1228 puede influir en la (re)selección de la UPF y el enrutamiento del tráfico. Basado en el despliegue del operador, cuando la AF 1228 se considera una entidad confiable, el operador de red puede permitir a la AF 1228 interactuar directamente con las NF relevantes. Además, la AF 1228 puede mostrar una interfaz basada en el servicio de Naf.

La NSSF 1229 puede seleccionar un conjunto de instancias de segmentos de red que sirve al UE 1201. La NSSF 1229 también puede determinar la NSSAI permitida y el mapeo a las S-NSSAI suscritas, si es necesario. La NSSF 1229 también puede determinar el conjunto de AMF que se usará para servir al UE 1201, o una lista de la(s) AMF candidata(s) 1221 basada(s) en una configuración adecuada y posiblemente consultando con la NRF 1225. La selección de un conjunto de instancias de segmentos de red para el UE 1201 puede activarse por la AMF 1221 con la que se registró el UE 1201 al interactuar con la NSSF 1229, lo que puede provocar un cambio de AMF 1221. La NSSF 1229 puede interactuar con la AMF 1221 a través de un punto de referencia N22 entre la AMF 1221 y la NSSF 1229; y puede comunicarse con otra NSSF 1229 en una red visitada a través de un punto de referencia N31 (no se muestra en la Figura 12). Además, la NSSF 1229 puede mostrar una interfaz basada en el servicio de Nnssf.

Como se describió anteriormente, la CN 1220 puede incluir una SMSF, que puede ser responsable de la comprobación y verificación de la suscripción de SMS, y de la

transmisión de mensajes SM para el/del UE 1201 para/de otras entidades, tales como un SMS-GMSC/IWMSC/SMS-router. El SMS también puede interactuar con la AMF 1221 y la UDM 1227 para un procedimiento de notificación de que el UE 1201 está disponible para la transferencia de SMS (p. ej., establecer un indicador de UE no accesible, y
 5 notificar a la UDM 1227 cuando el UE 1201 está disponible para el SMS).

La CN 1220 también puede incluir otros elementos que no se muestran en la Figura 12, tales como un sistema/arquitectura de almacenamiento de datos, un 5G-EIR, un SEPP y lo similar. El sistema de almacenamiento de datos puede incluir una SDSF, una UDSF y/o lo similar. Cualquier NF puede almacenar y recuperar datos no estructurados en/desde la UDSF (p. ej.,
 10 contextos de UE), a través del punto de referencia N18 entre cualquier NF y la UDSF (no se muestra en la Figura 12). Las NF individuales pueden compartir una UDSF para almacenar sus respectivos datos no estructurados o las NF individuales pueden tener cada una propia UDSF ubicada en o cerca de las NF individuales. Además, la UDSF puede mostrar una interfaz basada en el servicio Nudsf (no se muestra en la Figura 12). Los 5G-EIR pueden ser una NF
 15 que verifica el estado de PEI para determinar si los equipos/entidades particulares están desprovistos de la red; y el SEPP puede ser un indicador no transparente que realiza el ocultamiento de topología, filtrado de mensajes y control de políticas en interfaces de plano de control inter-PLMN.

Además, puede haber muchos más puntos de referencia y/o interfaces de servicio entre los
 20 servicios de NF en las NF; sin embargo, estas interfaces y puntos de referencia se han omitido de la Figura 12 para mayor claridad. En un ejemplo, la CN 1220 puede incluir una interfaz Nx, que es una interfaz inter-CN entre el MME (p. ej., MME XR121) y la AMF 1221 para permitir el interfuncionamiento entre la CN 1220 y CN XR120. Otros ejemplos de interfaces/puntos de referencia pueden incluir una interfaz basada en el servicio de N5g-EIR mostrada por un 5G-
 25 EIR, un punto de referencia N27 entre la NRF en la red visitada y la NRF en la red doméstica; y un punto de referencia N31 entre la NSSF en la red visitada y la NSF en la red doméstica.

Diversos componentes pueden describirse como que realizan una tarea o tareas, por conveniencia en la descripción. Debe interpretarse que tales descripciones incluyen la frase “configurado para”. La mención de un componente que se configura para realizar una o más tareas pretende expresamente que no se aplique la interpretación de 35 U.S.C.

5 § 112 (f) para ese componente.

Para una o más modalidades, al menos uno de los componentes establecidos en una o más de las figuras anteriores puede configurarse para realizar una o más operaciones, técnicas, procesos, o métodos como se expone en la sección ilustrativa a continuación. Por ejemplo, el sistema de circuitos de banda base como se describió anteriormente en conexión con una o

10 más de las figuras anteriores puede configurarse para operar de acuerdo con uno o más de los ejemplos expuestos a continuación. Para otro ejemplo, el sistema de circuitos asociado con un UE, estación base, elemento de red, etc., como se describió anteriormente en conexión con una o más de las figuras anteriores puede configurarse para operar de acuerdo con uno o más de los ejemplos expuestos a continuación en la sección ilustrativa.

15

Ejemplos

Se proporcionan en las siguientes secciones modalidades ilustrativas adicionales.

El Ejemplo 1 incluye una red personal de Internet de las cosas (IoT) (PIN) que se opera en cooperación con un sistema de comunicación inalámbrica asociado.

20 El Ejemplo 2 es la PIN del Ejemplo 1, en donde el sistema de comunicación inalámbrica asociado es un Sistema de 5.^a generación (5GS).

El Ejemplo 3 es la PIN del Ejemplo 1, en donde la red es una red doméstica inteligente o una red de dispositivos usables.

El Ejemplo 4 es la PIN del Ejemplo 1, en donde la red incluye una pluralidad de elementos.

25 El Ejemplo 5 es la PIN del Ejemplo 4, en donde al menos uno de la pluralidad de elementos es parte de más de una PIN.

El Ejemplo 6 es la PIN del Ejemplo 4, en donde la pluralidad de elementos incluye un dispositivo basado en 3GPP.

El Ejemplo 7 es la PIN del Ejemplo 5, en donde el dispositivo basado en 3GPP sirve como una puerta de enlace entre la PIN y los sistemas externos.

5 El Ejemplo 8 es la PIN del Ejemplo 1, en donde la PIN es creada por un usuario.

El Ejemplo 9 es la PIN del Ejemplo 1, en donde la PIN es creada por el sistema de comunicación inalámbrica asociado.

El Ejemplo 10 es la PIN del Ejemplo 1, en donde la PIN se crea mediante una función de aplicación (AF) dedicada a las PIN.

10 El Ejemplo 11 es la PIN del Ejemplo 1, en donde el sistema de comunicación inalámbrica asociado también gestiona el suministro de políticas de PIN, la autenticación de elementos y la incorporación de elementos para la PIN.

El Ejemplo 12 es la PIN del Ejemplo 1, en donde se asigna a la PIN uno o más atributos.

El Ejemplo 13 es la PIN del Ejemplo 12, en donde los atributos de PIN incluyen una clase PIN,
15 un alcance de tráfico de PIN, una clase de tráfico de PIN y un tamaño de PIN.

El Ejemplo 14 es la PIN del Ejemplo 13, en donde las categorías dentro de la clase PIN incluyen una PIN privada, una PIN pública y una PIN de área corporal personal, en donde las categorías dentro del alcance de tráfico de PIN incluyen: local, parcialmente local y en la nube, en donde las categorías dentro de la clase de tráfico de PIN incluyen tráfico de
20 alta prioridad y tráfico de baja prioridad, y en donde el tamaño de PIN es un número de elementos, una carga añadida de PIN, o un ciclo de trabajo de los elementos de PIN.

El Ejemplo 15 es la PIN del Ejemplo 13, los elementos de PIN se configuran con una capa de PIN que sirve como una interfaz común para intercambiar información entre los elementos.

25 El Ejemplo 16 es la PIN del Ejemplo 1, en donde el sistema de comunicación inalámbrica almacenó datos de suscripción del UE para un UE de PIN, y en donde los datos de suscripción del UE incluyen (i) una autorización para actuar como un PEGC y/o un PEMC, y/o (ii)

información que indica si se permite al UE solicitar dinámicamente la creación de un nuevo PIN.

El Ejemplo 17 es la PIN del Ejemplo 1, en donde la autorización para actuar como PEGC y/o PEMC es una autorización abierta o es una autorización restringida.

- 5 El Ejemplo 18 es un método para un equipo de usuario (UE), el método que comprende: generar una solicitud de registro que comprende una capacidad del UE para servir como una puerta de enlace para una red personal de Internet de las cosas (PIN); enviar la solicitud de registro a una estación base que sirve al UE; recibir, de la estación base, un mensaje de aceptación de registro que comprende una autorización de puerta de enlace
- 10 de PIN; e iniciar el establecimiento de PIN con al menos otro dispositivo, en donde el UE sirve como la puerta de enlace de PIN a la estación base.

El Ejemplo 19 es el método del Ejemplo 18, en donde la solicitud de registro comprende además uno o más atributos de PIN.

- El Ejemplo 20 es el método del Ejemplo 19, en donde el uno o más atributos de PIN
- 15 comprenden al menos uno de: una clase de PIN, un alcance de tráfico de PIN que proporciona una ubicación de tráfico de PIN, una clase de tráfico de PIN o un tamaño de PIN.

- El Ejemplo 21 es el método del Ejemplo 17, el método que comprende además: recibir, de la estación base, un contenedor de políticas de UE que comprende al menos uno de:
- 20 un identificador de PIN, una indicación de si informar el establecimiento de PIN a la estación base, o las reglas de la política de selección de ruta del UE (URSP) para el tráfico de PIN.

- El Ejemplo 22 es el método del Ejemplo 17, el método que comprende además transmitir una solicitud de establecimiento de PIN a la estación base; recibir un mensaje de
- 25 aceptación de establecimiento de PIN de la estación base; y completar de manera responsiva el establecimiento de PIN.

El Ejemplo 23 es el método del Ejemplo 22, en donde la solicitud de establecimiento de PIN comprende al menos uno de un identificador de PIN o un identificador del UE, y el mensaje de aceptación de establecimiento de PIN comprende al menos una de una duración de PIN o una restricción de ubicación.

- 5 El ejemplo 24 es el método del ejemplo 17, el método comprende además: recibir el tráfico de la aplicación del al menos otro dispositivo; determinar las reglas de la política de selección de ruta del UE (URSP) para el tráfico de la aplicación; y basado en las reglas de la URSP, iniciar el establecimiento de una sesión de unidad de datos de protocolo (PDU) para enrutar el tráfico de la aplicación.
- 10 El Ejemplo 25 es el método del Ejemplo 17, el método que comprende además: transmitir una solicitud de suministro de políticas de UE a la estación base; y recibir un comando de políticas de UE de la estación base, en donde el comando de políticas de UE comprende al menos uno de: un identificador de PIN, una indicación de si informar el establecimiento de PIN a la estación base, o las reglas de la política de selección de ruta del UE (URSP) para el tráfico de PIN.
- 15 El Ejemplo 26 es el método del Ejemplo 25, en donde la transmisión de la solicitud de suministro de políticas de UE se realiza en respuesta a la determinación de que el UE no tiene políticas válidas para la PIN.
- El Ejemplo 27 es el método del Ejemplo 17, el método que comprende además: transmitir, a través de la señalización de la capa de aplicación, información de PIN a una función de aplicación (AF) de PIN; y recibir, de la estación base, un contenedor de políticas de UE
- 20 que comprende al menos uno de: un identificador de PIN, una indicación de si informar el establecimiento de PIN a la estación base, o las reglas de la política de selección de ruta del UE (URSP) para el tráfico de PIN, en donde las reglas de la URSP se basan en la información de PIN.
- 25 El ejemplo 28 es el método del ejemplo 17, el método comprende además: recibir el tráfico de la aplicación del al menos otro dispositivo; determinar las reglas de la política de selección de ruta del UE (URSP) para el tráfico de PIN; y basado en las reglas de la URSP,

determinar el establecimiento de una nueva sesión de unidad de datos de protocolo (PDU) con configuraciones de PIN especificadas, las configuraciones de PIN especificadas que comprenden un nombre de red de datos (DNN) dedicado y una información de asistente de selección de segmentos de red de servicio (S-NSSAI); y transmitir una solicitud de establecimiento de sesión de PDU a la estación base.

El Ejemplo 29 es un método que comprende: recibir, de un equipo de usuario (UE), una solicitud de registro que comprende una capacidad del UE para servir como una puerta de enlace para una red personal de Internet de las cosas (PIN); determinar, basado en los datos de suscripción para el UE, que se autoriza al UE a servir como la puerta de enlace para la PIN; y transmitir, al UE, un mensaje de aceptación de registro que comprende una autorización de puerta de enlace de PIN.

El Ejemplo 30 es el método del Ejemplo 29, el método comprende además: determinar, basado en los datos de suscripción para el UE, una o más políticas de PIN para la PIN; y transmitir la una o más políticas de PIN al UE.

El Ejemplo 31 es el método del Ejemplo 30, en donde la una o más políticas de PIN comprenden al menos uno de: un identificador de PIN, una indicación de si informar el establecimiento de PIN a la estación base, o las reglas de la política de selección de ruta del UE (URSP) para el tráfico de PIN.

El Ejemplo 32 es el método del Ejemplo 30, en donde la una o más políticas de PIN se reciben de una función de aplicación (AF) de PIN.

El Ejemplo 33 es el método del Ejemplo 30, en donde la una o más políticas de PIN son políticas de PIN predeterminadas.

El Ejemplo 34 es el método del Ejemplo 29, el método que comprende además: recibir una solicitud de establecimiento de PIN del UE, la solicitud de establecimiento de PIN que comprende un identificador de PIN y un identificador de UE; suministrar, basado en los datos de suscripción para el UE, una o más restricciones para la PIN; y comunicar un mensaje de

aceptación de establecimiento de PIN al UE, el mensaje de aceptación de establecimiento de PIN que comprende una o más restricciones para la PIN.

El Ejemplo 35 es el método del Ejemplo 34, el método que comprende además: en respuesta a la recepción de la solicitud de establecimiento de PIN, activar una notificación de exposición de eventos a una función de aplicación (AF) de PIN; recibir una o más políticas de PIN de la AF de PIN; determinar, basado en la una o más políticas, una actualización de políticas de PIN para proporcionar al UE; y comunicar la actualización de políticas de PIN al UE.

El Ejemplo 36 es el método del Ejemplo 29, el método que comprende además: recibir, del UE, una solicitud para establecer una nueva sesión de unidad de datos de protocolo (PDU), la solicitud que comprende un nombre de red de datos (DNN) dedicado y una información de asistente de selección de segmentos de red de servicio (S-NSSAI); determinar, basado en una o más políticas de gestión de sesión (SM), que se permite al UE establecer la nueva sesión de PDU en un tiempo actual y una ubicación de UE actual; y comunicarse con una función de aplicación (AF) de PIN para realizar la autenticación y autorización secundarias de la solicitud para establecer la nueva sesión de PDU, en donde la AF de PIN sirve como una entidad de autenticación, autorización, contabilidad (AAA) de red de datos (DN).

El Ejemplo 37 incluye una función de aplicación (AF) personal de Internet de las cosas (PIN).

El Ejemplo 38 es la AF de PIN del Ejemplo 37, en donde la AF de PIN es una AF de PIN de operador de red móvil (MNO) o una AF de PIN de terceros.

El Ejemplo 39 es la AF de PIN del Ejemplo 37, en donde la AF de PIN crea políticas específicas para una PIN.

El Ejemplo 40 es la AF de PIN del Ejemplo 39, en donde la AF de PIN proporciona las políticas para el almacenamiento en una función de control de políticas (PCF).

El Ejemplo 41 es la AF de PIN del Ejemplo 39, en donde las políticas de PIN incluyen selección de ruta, información sobre el tamaño de PIN (p. ej. un número máximo de dispositivos), restricciones de tiempo y/o ubicación, y/o una indicación de si el 5GS tiene que participar en la creación de PIN.

El Ejemplo 42 es la AF de PIN del Ejemplo 37, en donde la AF de PIN es responsable de suministrar parámetros de PIN a una red central de un sistema de comunicación inalámbrica asociado.

El Ejemplo 43 es la AF de PIN del Ejemplo 42, en donde los parámetros de PIN incluyen tamaño de red, rendimiento y/o capacidad.

El Ejemplo 44 es la AF de PIN del Ejemplo 37, en donde la AF de PIN se suscribe para recibir notificaciones relacionadas con las PIN de un sistema de comunicación inalámbrica asociado.

El Ejemplo 45 es la AF de PIN del Ejemplo 37, en donde la AF de PIN inicia el suministro de parámetros de PIN.

El Ejemplo 46 es la AF de PIN del Ejemplo 45, en donde la AF de PIN que inicia el suministro de parámetros de PIN implica que la AF de PIN invoca un mensaje Nnef_ParameterProvision_Create para un nuevo evento de creación de PIN, el mensaje Nnef_ParameterProvision_Create enviado a una función de exposición de red (NEF).

El Ejemplo 47 es la AF de PIN del Ejemplo 46, en donde la AF de PIN incluye parámetros de políticas de PIN en el mensaje invocado que se envía a la NEF.

El Ejemplo 48 es la AF de PIN del Ejemplo 37, en donde la AF de PIN se suscribe a la notificación de parámetros de PIN.

El Ejemplo 49 es la AF de PIN del Ejemplo 48, en donde la AF de PIN invoca un mensaje Nnef_EventExposure_Subscribe para un nuevo evento de creación de PIN, el mensaje Nnef_EventExposure_Subscribe enviado a una función de exposición de red (NEF).

El Ejemplo 50 es la AF de PIN del Ejemplo 49, en donde la AF de PIN incluye características de PIN en el mensaje invocado que se envía a la NEF.

El Ejemplo 51 es la AF de PIN del Ejemplo 37, en donde la AF de PIN actúa como una entidad de autenticación, autorización, contabilidad (AAA) de red de datos (DN), para realizar la autenticación y autorización secundarias.

El Ejemplo 52 es la AF de PIN del Ejemplo 51, en donde la AF de PIN recibe, de una función de gestión de sesión (SMF), una solicitud para autorizar una nueva sesión de unidad de datos de protocolo (PDU).

El Ejemplo 53 es la AF de PIN del Ejemplo 52, en donde la AF de PIN realiza la autenticación y autorización secundarias en respuesta a la recepción de la solicitud.

El Ejemplo 54 es la AF de PIN del Ejemplo 37, en donde la AF de PIN intercambia información de PIN con un equipo de usuario (UE) de una PIN.

El Ejemplo 55 es la AF de PIN del Ejemplo 54, en donde la AF de PIN intercambia la información de PIN usando la señalización de la capa de aplicación.

El Ejemplo 56 es la AF de PIN del Ejemplo 54, en donde la información de PIN incluye las políticas de PIN del UE.

El Ejemplo 57 es la AF de PIN del Ejemplo 37, en donde la AF de PIN recibe un mensaje de exposición de eventos indicativo de una creación de PIN, el mensaje de exposición de eventos que incluye un nuevo evento de creación de PIN con un ID único.

El Ejemplo 58 es la AF de PIN del Ejemplo 57, en donde, en respuesta a la recepción del mensaje de exposición de eventos, la AF de PIN decide sobre las políticas de PIN para la PIN creada; y suministra políticas de PIN específicas para la PIN.

El Ejemplo 59 es la AF de PIN del Ejemplo 57, en donde, en respuesta a la recepción del mensaje de exposición de eventos, la AF de PIN asigna un identificador de PIN a la PIN creada y/o proporciona restricciones de PIN para la PIN creada.

El Ejemplo 60 incluye una función de gestión de sesión (SMF) de una red central de un sistema de comunicación inalámbrica.

El Ejemplo 61 es la SMF del Ejemplo 60, en donde, la SMF se configura para: recibir, de una función de gestión de acceso y movilidad (AMF, en inglés), una solicitud de información de suscripción de un equipo de usuario (UE), la información de suscripción que indica si el UE tiene capacidad de gestión activa (PEMC) y/o una capacidad de puerta de enlace activa (PEGC); y proporcionar la información de suscripción a la AMF.

El Ejemplo 62 es la SMF del Ejemplo 60, en donde la SMF se configura para: obtener políticas de gestión de sesión (SM) aplicables a una red personal de Internet de las cosas (IoT) (PIN); y enrutar el tráfico de PIN basado en las políticas de SM.

El Ejemplo 63 es la SMF del Ejemplo 60, en donde la SMF se configura para: recibir una solicitud de establecimiento de sesión de PDU de un equipo de usuario (UE); evaluar si se le permite establecer la sesión de PDU en un tiempo actual y desde una ubicación del UE; y, en respuesta a la determinación de que se le permite hacerlo, contactar a una función de aplicación de PIN para una autorización secundaria.

El Ejemplo 64 incluye una función de control de políticas de una red central de un sistema de comunicación inalámbrica.

El Ejemplo 65 es la PCF del Ejemplo 64, en donde la PCF se configura con políticas predeterminadas para configuraciones de red personal de Internet de las cosas (PIN).

El Ejemplo 66 es la PCF del Ejemplo 64, en donde la PCF recibe políticas de red personal de Internet de las cosas (PIN) de una función de aplicación (AF) de PIN y/o de una gestión unificada de datos (UDM, en inglés).

El Ejemplo 67 es la PCF del Ejemplo 66, en donde la PCF consulta a la UDM para recuperar una o más políticas de PIN aplicables a una suscripción de un equipo de usuario (UE).

El Ejemplo 68 es la PCF del Ejemplo 67, en donde la PCF envía instrucciones a una función de gestión de acceso y movilidad (AMF) para proporcionar una o más políticas de PIN al UE.

El Ejemplo 69 es la PCF del Ejemplo 66, en donde la PCF recibe una solicitud de políticas de PIN de un equipo de usuario (UE).

El Ejemplo 69 es la PCF del Ejemplo 66, en donde la PCF envía una actualización de política a una AMF, en donde las políticas de PIN incluyen un identificador de PIN y/o las reglas de la URSP para el tráfico de PIN.

El Ejemplo 70 es una gestión unificada de datos (UDM) de una red central de un sistema de comunicación inalámbrica.

El Ejemplo 71 es la UDM del Ejemplo 70, en donde la UDM almacena datos de suscripción del UE, que pueden incluir la autorización de un UE para actuar como un PEGC y/o un PEMC.

El Ejemplo 72 es la UDM del Ejemplo 70, en donde la UDM almacena una o más políticas para las PIN.

- 5 El Ejemplo 73 puede incluir uno o más medios no transitorios legibles por computadora que comprenden instrucciones para hacer que un dispositivo electrónico, después de la ejecución de las instrucciones por uno o más procesadores del dispositivo electrónico, realice uno o más elementos de un método descrito en o relacionado con cualquiera de los Ejemplos 1-72, o cualquier otro método o proceso descrito en la presente descripción.
- 10 El Ejemplo 74 puede incluir un aparato que comprende lógica, módulos o sistema de circuitos para realizar uno o más elementos de un método descrito en o relacionado con cualquiera de los Ejemplos 1-72, o cualquier otro método o proceso descrito en la presente descripción.
- El Ejemplo 75 puede incluir un método, técnica, o proceso como se describe en o se relaciona con cualquiera de los Ejemplos 1-72, o porciones o partes de estos.
- 15 El Ejemplo 76 puede incluir un aparato que comprende: uno o más procesadores y uno o más medios legibles por computadora que comprenden instrucciones que, cuando se ejecutan por el uno o más procesadores, hacen que el uno o más procesadores realicen el método, técnicas o proceso como se describe en o se relaciona con cualquiera de los Ejemplos 1-72, o porciones de estos.
- 20 El Ejemplo 77 puede incluir una señal como se describe en o se relaciona con cualquiera de los Ejemplos 1-72, o porciones o partes de estos.
- El Ejemplo 78 puede incluir un datagrama, elemento de información, paquete, trama, segmento, PDU o mensaje como se describe en o se relaciona con cualquiera de los Ejemplos 1-72, o porciones o partes de estos, o descritos de cualquiera otra manera en la
- 25 presente descripción.

El Ejemplo 79 puede incluir una señal codificada con datos como se describe en o se relaciona con cualquiera de los Ejemplos 1-72, o porciones o partes de estos, o descritos de cualquier otra manera en la presente descripción.

5 El Ejemplo 80 puede incluir una señal codificada con un datagrama, IE, paquete, trama, segmento, PDU o mensaje como se describe en o se relaciona con cualquiera de los Ejemplos 1-72, o porciones o partes de estos, o descritos de cualquiera otra manera en la presente descripción.

10 El Ejemplo 81 puede incluir una señal electromagnética que transporta instrucciones legibles por computadora, en donde la ejecución de las instrucciones legibles por computadora por uno o más procesadores hace que uno o más procesadores realicen el método, técnicas o proceso como se describe o se relaciona con cualquiera de los Ejemplos 1-72, o porciones de estos.

15 El Ejemplo 82 puede incluir un programa informático que comprende instrucciones, en donde la ejecución del programa por un elemento de procesamiento es hacer que el elemento de procesamiento realice el método, técnicas o proceso como se describe en o se relaciona con cualquiera de los Ejemplos 1-72, o porciones de estos.

El Ejemplo 83 puede incluir una señal en una red inalámbrica como se muestra y describe en la presente descripción.

20 El Ejemplo 84 puede incluir un método de comunicación en una red inalámbrica como se muestra y describe en la presente descripción.

El Ejemplo 85 puede incluir un sistema para proporcionar comunicación inalámbrica como se muestra y describe en la presente descripción.

El Ejemplo 86 puede incluir un dispositivo para proporcionar comunicación inalámbrica como se muestra y describe en la presente descripción.

25 Cualquiera de los ejemplos descritos anteriormente puede combinarse con cualquier otro ejemplo (o combinación de ejemplos), a menos que se indique explícitamente de cualquier otra manera. La descripción anterior de una o más implementaciones

proporciona ilustración y descripción, pero no pretende ser exhaustiva ni limitar el alcance de las modalidades a la forma precisa descrita. Las modificaciones y variaciones son posibles a la luz de las enseñanzas anteriores o pueden adquirirse a partir de la práctica de diversas modalidades.

5 Como se describió anteriormente, un aspecto de la presente tecnología puede relacionarse con la recolección y el uso de datos disponibles de fuentes específicas y legítimas para permitir la interacción con un segundo dispositivo para una transferencia de datos. La presente descripción contempla que, en algunos casos, este dato recopilado puede incluir datos de información personal que identifican o pueden usarse de manera única para
10 identificar una persona específica. Tales datos de información personal pueden incluir datos demográficos, datos basados en ubicación, identificadores en línea, números telefónicos, direcciones de correo electrónico, direcciones de hogar, datos o registros relacionados con la salud o nivel de bienestar físico de un usuario (p. ej., mediciones de signos vitales, información de medicación, información de ejercicios), fecha de nacimiento,
15 o cualquier otra información personal.

La presente descripción reconoce que el uso de tales datos de información personal, en la presente tecnología, puede usarse para el beneficio de los usuarios. Por ejemplo, los datos de información personal pueden usarse para proporcionar transferencias de datos seguras que se realizan entre un primer dispositivo y un segundo dispositivo. Los datos de
20 información personal pueden utilizarse además para identificar una cuenta asociada con el usuario desde un proveedor de servicio para completar una transferencia de datos.

La presente descripción contempla que aquellas entidades responsables de la recolección, análisis, descripción, transferencia, almacenamiento, u otro uso de tales datos de información personal cumplen con las políticas de privacidad y/o prácticas de
25 privacidad bien establecidas. En particular, se esperaría que tales entidades implementen y apliquen consistentemente prácticas de privacidad que se reconocen generalmente como que cumplen o superan los requisitos de la industria o gubernamentales para

mantener la privacidad de los usuarios. Tal información relacionada con el uso de datos personales deberá ser prominente y fácilmente accesible por los usuarios, y deberá actualizarse a medida que la recolección y/o el uso de datos cambia. La información personal de los usuarios deberá recolectarse solo para usos legítimos. Además, tal

5 recolección/intercambio deberá ocurrir solo después de recibir el consentimiento de los usuarios u otra base legítima especificada en la ley aplicable. Además, tales entidades deberán considerar tomar cualquier medida necesaria para proteger y asegurar el acceso a tales datos de información personal y garantizar que otros con acceso a los datos de información personal se adhieran a sus políticas y procedimientos de privacidad.

10 Además, tales entidades pueden someterse a sí mismas a la evaluación por parte de terceros para certificar su adherencia a políticas y prácticas de privacidad ampliamente aceptadas. Además, las políticas y prácticas deben adaptarse para los tipos particulares de datos de información personal que se recopilan y/o acceden y se adaptan a las leyes y normas aplicables, incluidas las consideraciones específicas de una jurisdicción que

15 pueden servir para imponer un estándar más alto. Por ejemplo, en los EE. UU., la recolección o el acceso a ciertos datos de salud pueden estar regulados por leyes federales y/o estatales, tales como la Ley de Portabilidad y Responsabilidad del Seguro de Salud (HIPAA, en inglés); mientras que los datos de salud en otros países pueden estar sujetos a otras regulaciones y políticas y deben manejarse en consecuencia.

20 A pesar de lo anterior, la presente descripción contempla también modalidades en las que los usuarios bloquean selectivamente el uso de, o acceso a, datos de información personal. Es decir, la presente descripción contempla que elementos de hardware y/o software pueden proporcionarse para evitar o bloquear el acceso a tales datos de información personal. Por ejemplo, la presente tecnología puede configurarse para permitir a los usuarios seleccionar

25 “aceptar” o “no aceptar” su participación en la recolección de datos de información personal durante el registro para servicios o en cualquier momento posterior. Por ejemplo, un usuario puede “aceptar” o “no aceptar” tener información asociada con una cuenta del usuario

almacenada en un dispositivo de usuario y/o compartido por el dispositivo de usuario. Además de proporcionar las opciones de “aceptar” y “no aceptar”, la presente descripción contempla proporcionar notificaciones relacionadas con el acceso o uso de información personal. Por ejemplo, puede notificarse a un usuario al descargar una solicitud que se va a acceder a sus datos de información personal y después recordárselo nuevamente justo antes de que la aplicación acceda a los datos de información personal. En algunos casos, puede notificarse al usuario al inicio de una transferencia de datos del dispositivo que accede a información asociada con la cuenta del usuario y/o al compartir información asociada con la cuenta del usuario con otro dispositivo.

Además, es la intención de la presente descripción que los datos de información personal deben manejarse y gestionarse en una manera que minimice los riesgos de acceso o uso involuntario o no autorizado. El riesgo puede minimizarse limitando la recolección de datos y eliminando datos una vez que ya no sean necesarios. Además, y cuando sea aplicable, incluso en determinadas solicitudes relacionadas con la salud, puede usarse la desidentificación de datos para proteger la privacidad de un usuario. La desidentificación puede facilitarse, cuando sea apropiado, eliminando identificadores, controlando la cantidad o especificidad de los datos almacenados (p. ej., recolectando datos de ubicación a nivel de la ciudad en lugar de a nivel de dirección), controlando cómo se almacenan los datos (p. ej., añadiendo datos a través de usuarios), y/u otros métodos tales como la privacidad diferencial.

Por lo tanto, aunque la presente descripción cubre ampliamente el uso de datos de información personal para implementar una o más diversas modalidades descritas, la presente descripción también contempla que las diversas modalidades pueden implementarse también sin la necesidad de acceder a tales datos de información personal. Es decir, las diversas modalidades de la presente tecnología no se vuelven inoperables debido a la falta de la totalidad o una parte de tales datos de información personal. Por ejemplo, el contenido puede seleccionarse y suministrarse a los usuarios basado en datos de información no personal añadidos o una cantidad mínima de

información personal, tal como el contenido que se maneja solo en el dispositivo del usuario u otra información no personal disponible para los servicios de suministro de contenido.

5 Aunque las modalidades anteriores han sido descritas en detalle considerable, numerosas variaciones y modificaciones serán evidentes para los expertos en la técnica una vez que la descripción anterior se aprecia completamente. Se pretende que las siguientes reivindicaciones abarquen todas tales variaciones y modificaciones.